НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»
УДК 004.056

«До захисту допущено»
В.о. завідувача кафедри
_____ М.В.Грайворонський
“___”_____2018 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему: Математичні методи оцінки ризиків для процедур телемедицини в Україні

Виконав (-ла): студент (-ка) 2 курсу, групи ФБ-71мп
(шифр групи)

Авдєєва Людмила Костянтинівна
(прізвище, ім’я, по батькові)

Науковий керівник к.т.н., доцент Литвинова Тетяна Василівна _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент к.ф.-м.н., доцент Шраменко В.М. _ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою
Спеціальність (спеціалізація) – 125 Кібербезпека («Системи і технології кібербезпеки)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)

«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Авдєєва Людмила Костянтинівна

1. Тема дисертації: Математичні методи оцінки ризиків для процедур телемедицини в Україні
науковий керівник дисертації к.т.н., доцент Литвинова Тетяна Василівна,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «15» листопада 2018 р. № 4171-с

2. Термін подання студентом дисертації 12.12.2018 р.

3. Об'єкт дослідження _____
_____

4. Вихідні дані _____
_____
_____
_____

5. Перелік завдань, які потрібно розробити _____
_____
_____
_____
_____
_____

6. Орієнтовний перелік ілюстративного матеріалу _____
_____
_____

7. Орієнтовний перелік публікацій _____
_____

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка

Студент _____ (підпис) _____ (ініціали, прізвище)

Науковий керівник дисертації _____ (підпис) _____ (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Робота обсягом 105 сторінки містить 6 ілюстрацій, 47 таблиць та 14 літературних посилань.

Метою даної кваліфікаційної роботи є дослідження телемедицини та людини як складової частини системи телемедицини.

Об'єктом дослідження є людина та все що пов'язано з нею у рамках телемедицини.

Предметом дослідження є ризики для людини в телемедицині в контексті інформаційної безпеки.

Результати роботи викладені у вигляді таблиці та методу, що дозволяє проводити різносторонню оцінку ризиків інформаційної безпеки для телемедицини.

Результати роботи можуть бути використані при розробці математичних формалізованих методів оцінки ризиків телемедичних процедур. Також можна використовувати представлений метод для оцінки існуючих моделей безпеки телемедицини та порівняння з результатами оцінки безпеки в інших галузях.

РИЗИК, УРАЗЛИВІСТЬ, ТЕЛЕМЕДИЦИНА, БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ, МАТЕМАТИЧНІ МЕТОДИ ОЦІНКИ РИЗИКІВ

ABSTRACT

The work includes 105 pages, 6 figures, 47 tables and 14 literary references.

The aim of this qualification is to research telemedicine and humans as part of the telemedicine system.

The object of researches is human and everything connected with it within the framework of telemedicine.

The subject of research is the risks to humans in telemedicine in context of information security.

The results are presented in the form of a table and method that allows us to carry out a comprehensive assessment of the risks of information security for telemedicine.

The results of work can be used in the development of mathematical formalized methods for assessing the risks of telemedicine procedures. Also can be uses to assess existing telemedicine security models and compare them with the results of safety assessment in other industries.

RISK, VULNERABILITY, TELEMEDICINE, SECURITY OF INFORMATION AND COMMUNICATION SYSTEMS, MATHEMATICAL METHODS OF RISK ASSESSMENT

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Телемедицина – комплекс організаційних, фінансових і технологічних заходів, що забезпечують надання дистанційної консультаційної медичної послуги, при якій пацієнт або лікар, що безпосередньо проводить обстеження та/або лікування пацієнта, отримує дистанційну консультацію іншого лікаря з використанням телекомунікацій. Телемедицина за означенням ВООЗ – це метод надання послуг з медичного обслуговування там, де відстань є критичним фактором [1].

Телемедичні послуги – дистанційні медичні консультації, консиліуми, контроль фізіологічних параметрів організму пацієнта, проведення діагностичних і лікувальних маніпуляцій, обмін результатами обстеження пацієнта, інші медичні послуги, а також медичні відео конференції, медичні відео семінари, медичні відео лекції, що здійснюються у вигляді обміну електронними повідомленнями з використанням телекомунікацій [1].

Реалізація уразливості – будь-які дії, що спрямовано на порушення цілісності, доступності чи конфіденційності інформації, що циркулює в системі, використовуючи вразливість системи. Реалізація уразливості можлива не тільки для зловмисника, проте і для неперадбаченному збігу обставин, ненавмисних дій користувача системи. У комп'ютерній безпеці, уразливість (англ. system vulnerability) — нездатність системи протистояти реалізації певної загрози або сукупності загроз [2]. Для уразливості можливе проведення її реалізації.

Атака — детально підібраний набір дій, які, в разі успіху, призведуть або до пошкодження ресурсів веб-застосунку або до небажаної операції.

Cross-Site Scripting (XSS) — атака, що змушує веб-застосунки взаємодіяти з наданими користувачем даними як з виконуваними скриптами в веб-браузері користувача. При успішному виконанні атаки зловмисник може отримати доступ до всього контенту веб-браузера (Cookie, історію, версія програми тощо).

SQL ін'єкції — атака спрямована на введення на стороні клієнту SQL команд, що надсилаються на сервер для несанкціонованого виконання.

Метод «грубої сили» (від англ. Brute force; або повний перебір) — метод рішення криптографічної задачі шляхом перебору всіх можливих варіантів ключа. Складність повного перебору залежить від кількості всіх можливих рішень задачі. Якщо простір рішень дуже великий, то повний перебір може не дати результатів протягом декількох років або навіть століть.

XML eXternal Entity (XXE) Injection, XXE ін'єкція — це тип атаки на застосунок, яке аналізує ввід XML [3].

Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

Об'єкт ризику – це людина та все, що пов'язано з її існуванням та її діяльністю. Ризиковий стан – перелік можливих результатів з зазначенням їх ймовірностей

Загроза (англ. threat) — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають атакою.

ВСТУП

Актуальність роботи забезпечення більш надійного проведення телепроцедур, що розвиваються з великою швидкістю і можуть рятувати життя, популяризація телемедицини.

Мета і завдання дослідження провести дослідження процедур телемедицини, провести математичну оцінку ризиків у них.

Об'єкт дослідження: людина та все, що пов'язано з нею у рамках телемедицини.

Предмет дослідження: ризики для людини в телемедицині.

Метою роботи є дослідження ризиків для кінцевого споживача.

Методи дослідження математичні оцінки ризиків.

Наукова новизна одержаних результатів в тому, що на даний момент не існує єдиного підходу до тестування та розробки захисту ІБ на базі оцінки ризику як комплексного явища, що надає інформацію медичному персоналу щодо покращення стану ІБ та просування телемедицини.

Практичне значення одержаних результатів в тому, щоб наглядно показати медичному персоналу, що виконує телемедичні процедури, що результат їх дії напряму пов'язані з безпекою інформації, важливе не тільки нормативне ставлення, але й середовище, а також супровід.

1 ОГЛЯД ІСНУЮЧИХ ДАНИХ

1.1 Поняття телемедицини

Телемедици́на — напрямок медицини, що використовує телекомунікаційні й електронні інформаційні (комп'ютерні) технології для надання медичної допомоги й послуг у сфері охорони здоров'я в точці необхідності (у тих випадках, коли географічна відстань є критичним чинником) [4].

Ціль телемедицини — надання будь-якій людині, незалежно від її місцезнаходження, медичної допомоги в необхідному обсязі й в актуальний термін. Предмет телемедицини — обмін за допомогою телекомунікацій і комп'ютерних технологій всіма видами медичної інформації між віддаленими пунктами. При цьому даний процес обміну характеризується видом переданої інформації й способом її передачі. Функції телемедицини — клінічні, організаційно-адміністративні, превентивні, навчальні, наукові. Системи цифрових табло встановлюються не тільки на загальнодоступних ділянках різних клінік, а й в оглядових кабінетах, лабораторіях і операційних.

Галузевим нормативним документом з застосування телемедицини в Україні є Наказ МОЗ від 26.03.2010 № 261 «Про впровадження телемедицини в закладах охорони здоров'я» та методичні рекомендації.

В Україні у 2007 році створено Державний клінічний науково-практичний центр телемедицини МОЗ України — єдиний спеціалізований заклад охорони здоров'я, створений для впровадження та розвитку телемедицини в Україні. Постановою Кабінету Міністрів України від 01.10.2008 року № 878 його віднесено до Переліку закладів охорони здоров'я, що забезпечують виконання загальнодержавних функцій. Згідно Статуту, Державний центр телемедицини забезпечує надання висококваліфікованої комплексної консультативної медичної допомоги населенню із застосуванням телемедичних технологій [1].

Із 2009 року Державним центром телемедицини реалізується проект створення телемедичної мережі України, завдяки якій започатковано телемедичне консультування та обмін досвідом лікарів на Порталі телемедицини.

Телемедицина — це найширший спектр сучасних комп'ютерно-телекомунікаційних технологій, здебільшого простих й доступних будь-якому користувачеві. Зазвичай одну клінічну або організаційну задачу можливо вирішити принципово різними технічними засобами. Найчастіше зустрічається міф стосовно телемедицини — коли її технічний потенціал дорівнюють відеоконференсінгу або телеметричним пристроям тощо. Подібний підхід є помилковим. Менеджер системи охорони здоров'я повинен чітко визначити мету, оцінити економічні можливості, визначити ключові моменти процесів надання медико-санітарної допомоги, врахувати кадрові, соціальні, географічні та інші локальні особливості, а потім — обрати ті технічні рішення для побудови телемедичних систем, котрі будуть оптимальними для даних цілей та умов. Також важливим підґрунтям для побудови телемедичної інфраструктури є доказові дослідження та клінічні випробування.

Телемедична процедура — стандартна послідовність спільних дій зі строго певною метою географічно віддалених один від одного медпрацівників, пацієнта(ів) і допоміжного персоналу з використанням комп'ютерної й телекомунікаційної техніки.

Існуючі у наш час види телемедичних послуг можна умовно поділити на шість категорій, що становлять загальну телемедицину:

-телемедичне консультування;

-біотелеметрія (телемоніторинг);

-домашня (індивідуальна) телемедицина;

-телескринінг;

-телеприсутність/телеасистування;

-дистанційне навчання.

Також окрім шести телемедичних процедур існує телесестринство. Якщо телемедицина розуміє під собою допомогу лікаря-професіонала, чи спеціаліста, що має відповідну кваліфікацію, телесестринство дозволяє звичайній медсестрі, що не має відповідного диплома, проте має практичні навички, допомагати пацієнту так само, як і лікар у сенсі телемедицини.

Телемедсестринство (від англ. telenursing) - використання телекомунікацій і інформативних комп'ютерних технологій для надання сестринської допомоги і забезпечення координованої роботи медсестер у випадку, коли фізична відстань є критичним чинником.

Використовувати телемедсестринствао можливо амбулаторно, у лікарні, у телемедичному центрі або за допомогою мобільних пунктів.

Телемедсестринство використовує більшість технологій телемедицини і включає в себе комплекс послуг, що забезпечують комфорт не лише для пацієнта, але і для персоналу, допомагаючи у їх роботі.

Основні технології медсестринства:

-телефонний або відеоконференц-зв'язок між медичним центром та пацієнтом удома (дає змогу дивитися і коментувати перев'язки, маніпуляції, прийманням медикаментів, обгорювати лікування);

-сестринські телеконсультації (консультації за протоколом й алгоритмом у вигляді програм, сортування пацієнтів);

-дистанційне навчання пацієнтів і його родичів;

-телеконтроль і/або моніторинг діагностичних досліджувань;

- асистування лікареві в проведенні протоколу лікування;

-пересилання фізіологічних параметрів (артеріальний тиск, рівень глюкози крові, маса тіла, зріст) через Інтернет.

1.2 Аналіз складових частин телемедицини

Телемедицина, як і звичайна медицина, складається з багатьох частин, кожна з яких має свої особливості. І як і медицина, далеко не завжди можна чітко провести грань, де ж один з видів процедур перейшов в інший. Думки експертів з цього приводу розділяються, оскільки декотрі схильні розділяти телемедицину на сім чи навіть більше незалежних процедур, інші ж визнають лише три-чотири види і не більше. Далі буде представлено шість видів процедур, які автор виділив для себе і базуючись виключно на послугах та технологіях, які пропонуються телемедичними процедурами.

1.2.1 Телемедичне консультування

Найпоширенішою в даний час процедурою є телемедичне консультування (дистанційне обговорення клінічного випадку), яке забезпечує наближення кваліфікованої допомоги, швидку підтримку клінічних рішень та покращує якість та доступність медико-санітарної допомоги. Телемедичне консультування є компонентом повсякденної лікувально-діагностичної роботи. З метою отримання підтримки для прийняття оптимального клінічного рішення кожен лікар повинен володіти навичками з підготовки медичної інформації та проведення телемедичного консультування. Менеджер системи/закладу охорони здоров'я також повинен вільно володіти подібними навичками для підтримки власної лікувальної роботи, аудиту телемедичної діяльності, контролю інформаційної безпеки, забезпечення надання медичних послуг на сучасному рівні на основі доказової медицини. Додатково наголосимо, що обов'язковим компонентом діяльності сучасного лікаря є спілкування з колегами через Інтернет (тематичні списки розсилання, професійні Інтернет-товариства, соціальні мережі), що також

включає неформальне телеконсультування, яке здійснюється без протоколювання, але з дотриманням усіх вимог щодо якості та безпеки.

Телемедичне консультування перш за все здійснюється на основі різноманітних відео конференцій, розсилок листів через Інтернет та навіть звичайного дзвінка. Саме тому цей напрямок став таким популярним у наш час, та в Україні особливо.

При розгляді телемедичного консультування та захисті інформації у ньому перш за все увага акцентується на конфіденційності інформації та професійності лікарів.

Отже, увагу слід зосередити саме на захисті даних, що циркулюють у системі, залишивши на другому плані швидкість та безперервність каналу. Тут слід розуміти, що відповіді на листи не мають бути миттєвими, а виклик до телеконференції не є пріоритетним видом діяльності для лікаря на робочому місці.

1.2.2 Біотелеметрія (телемоніторинг)

Телеметрія — сукупність технічних засобів і методів вимірювання на відстані різних фізичних, технічних та інших величин у промислових, енергетичних, транспортних та інших установках. Передавання визначених даних з будь-якої точки на віддалений термінал [5].

Телеметрія у контексті телемедицини (дистанційна фіксація фізіологічних параметрів) виникла як компонент космічної медицини; а її цивільний різновид — телемоніторинг — використовується в відділеннях інтенсивної терапії та при транспортування важких пацієнтів. Саме телеметрія застосовується в військовій, аерокосмічній медицині та медицині катастроф. Найпоширенішою формою клінічного застосування телеметрії є теле-ЕКГ.

Перш за все, ця процедура призначена для діагностики стану хворого, де головними чинникам є точність та швидкість роботи обладнання. Головними факторами у даному виді процедур виступають саме точність, достовірність, безперервність та швидкість. На другий план відходять конфіденційність та спроможність даної системи проводити моніторинг на значних відстанях.

Як все було сказано, саме теле-ЕКГ є найпоширенішою фомою застосування, а в Україні це стало і одним з перших прикладів телемедицини взагалі.

Дана система підтримує життєздатність за допомогою комплексу програм, що поєднують датчики та термінали, на яких виводяться дані. Головна складова такої системи саме обладнання, оскільки програмний комплекс є досить простим і відіграє не таку важливу роль.

Також окремою частиною біотелеметрії слід вважати медицину катастроф, військову біотелеметрію та аерокосмічну медицину, де відстань вже займає одне з перших місць в списку пріоритетів, поруч з достовірністю та точністю. Дані системи обладнані складним комплексом програм та не менш складною технічною частиною, що є результатом роботи багатьох спеціалістів та великих затрат не тільки часу, але і коштів.

1.2.3 Домашня (індивідуальна) телемедицини

Навіть порівняно з іншими процедурами телемедицини, домашня або індивідуальна телемедицина є досить молодою галуззю, що швидко набуває популярності у наш час.

Телесестринство, телеконференції, телеконсультації, навіть деякі частини біотелеметрії. Домашня телемедицина включає в себе це все.

Перш за все, ця процедура націлена на людей, які через своє положення або стан здоров'я не бажають знаходитися у лікарні. Політики, різноманітні

знаменитості, тяжко хворі з постійним діагнозом, навіть люди похилого віку, які бажають провести решток життя з сім'єю, а не в лікарні. Також не слід забувати, що хоча у першу чергу індивідуальна телемедицина створювалася для таких випадків і була досить дорогим задоволенням, з розвитком технологій і плином часу, вона все більш стає народною.

Під цим слід розуміти, що зараз навіть середній клас населення може дозволити собі комп'ютер, а отже і долучитися до індивідуальної телемедицини.

Звісно, ця процедура перетинається, а інколи і захоплює у себе інші, проте головна її відзнака, те, що виділяє саме цей комплекс на фоні інших процедур, це націленість на єдину особу.

Здійснюється це за допомогою комплексу програм, в індивідуальних випадках – дорогого обладнання. В основному індивідуальна телемедицина потребує від пацієнта лише його власного бажання лікуватися вдома, а зовсім не коштів.

Головними характеристиками цієї процедури є конфіденційність, точність і доступність. Оскільки процедура має бути доступна цілодобово, має забезпечувати необхідний рівень медичної допомоги та дотримуватися медичних норм.

1.2.4 Телескринінг

Телескринінг (дистанційне виявлення й формування груп ризику, профілактичні дії з використанням телемедичних засобів) забезпечує широкий комплекс превентивних заходів, особливо актуальних для покращення здоров'я дітей та підлітків (розлади зору у немовлят, порушення постави у підлітків тощо), раннього виявлення онкологічної та фтизіатричної патології, особливо це стосується населення сільської місцевості, закритих колективів [5].

Перш за все, ця процедура націлена на превентивні заходи для покращення загального рівня медичної допомоги. Скринінг націлено на виявлення, а отже і

діагностування захворювань у ранній стадії, особливо коли пацієнт знаходиться на великій відстані від спеціаліста, що може провести правильне обстеження та поставити діагноз.

Дана процедура забезпечується за допомогою цілого комплексу, перш за все, апаратного. Окрім обладнання, що буде забезпечувати необхідне сканування, також телескринінг потребує програмного комплексу, що також поділяється на складові. Перша така складова – БД, де зберігається уся необхідна інформація. Друга – програми, що проводять первинну вибірку за рядом ознак, вказаних та затверджених відповідними спеціалістами.

Тут конфіденційність пацієнта хоча і є необхідною складовою, проте перш за все має бути точність та актуальність. Формування груп ризику та подальше їх дослідження відповідним спеціалістом – час і гроші, а іноді і життя. Програми мають працювати точно, інформація, що циркулює в них, має бути цілісною, а БД зберігати свою структуру та дані навіть у разі відмови інших систем.

1.2.5 Телеприсутність/телеасистування

Телеприсутність (з телеманіпулюванням) та індивідуальна телемедицина є нині основними трендами розвитку. Ці системи забезпечують постійне медичне спостереження та контроль за пацієнтами на амбулаторному етапі, повноцінну участь експерта в процесі надання медичної допомоги (особливо невідкладної) у віддаленому медичному закладі. Вище вказані телемедичні процедури забезпечують безперервність медико-санітарної допомоги та професійного навчання, також вони спрямовані на вирішення важливих кадрових та економічних проблем галузі охорони здоров'я.

Телеасистування – дистанційний синхронний супровід медичних маніпуляцій або дистанційне керування лікувальним та діагностичним обладнання [5].

Телеасистування та телеприсутність є не просто спорідненими процедурами, але й невід'ємними одна від одної, хоча деякі джерела схильні розділяти їх на окремі частини.

Перш за все, ці процедури є одними з найбільш перспективних напрямів розвитку, що в майбутньому дійсно зможуть зробити медичну допомогу доступною для усього населення планети.

Також доволі часто у сенсі телеасистування можна зустріти і доволі новий термін як телехірургія. Вони не є одним й тим самим, проте телехірургія є новим етапом розвитку телеасистування.

Це складні технології, що включають в себе не лише програмно-апаратний комплекс, проте і компетентний персонал, навчений працювати з даними технологіями.

Усі три процедури потребують безперервності каналу, швидкості, достовірності, точності та цілісності потоку інформації. Конфіденційність не є таким важливим пунктом, проте і вона відіграє значну роль.

1.2.6 Дистанційне навчання

Дистанційне навчання — сукупність сучасних технологій, що забезпечують доставку інформації в інтерактивному режимі за допомогою використання ІКТ (інформаційно-комунікаційних технологій) від тих, хто навчає (викладачів, визначних постатей у певних галузях науки, політиків), до тих, хто навчається (студентів чи слухачів). Основними принципами дистанційного навчання є інтерактивна взаємодія у процесі роботи, надання студентам можливості самостійного освоєння досліджуваного матеріалу, а також консультаційний супровід у процесі дослідницької діяльності. Дає змогу навчатися на відстані, за допомогою диспутів експертів із кількох країн, за відсутності викладача. Основну

роль у здійсненні дистанційного навчання відіграють сучасні інформаційні технології.

У сенсі телемедицини дистанційне навчання є складовою підготовки персоналу до проведення більш складних процедур у подальшому. Також окрім персоналу, що в обов'язковому порядку проходить такі курси та школи, дистанційно навчатися також можуть і пацієнти.

Її головним пріоритетом стають різноманітні превентивні заходи та процедури, які можна проводити вдома. Навчатися також можуть сім'ї пацієнтів, щоб допоїти хворому на етапі одужання чи супроводжувати його під час лікування.

Окрім спеціалізованих сайтів та програмних оболонок, на основі яких і проводиться навчання, частинами такого комплексу можуть виступати й загальні програми та сайти. Різні відео, аудіо та текстові документи, платформи, які дають до них доступ та інше.

Головними пунктами на даному етапі стають достовірність та актуальність наданої інформації. Час відіграє не таку важливу роль, як і конфіденційність користувачів.

1.3 Загрози для телемедицини

Загроза (англ. threat) — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають атакою.

З плином часу розвитку набувають не тільки технології, що спрямовані на покращення життя людей, проте і технології нападу. Не лише військові складова, війни 21 сторіччя вже не ведуться на полі бою, вони перемістилися на інші простори. І головним полем став Інтернет.

Як і в минулих сторіччях, медична допомога є складовою частиною будь-якої війни, і навіть коли вона надається мирному населенню у зоні бойових дій, лікарі

під загрозою. Так само відбувається і в Інтернеті. Хоча медична допомога та їх технології спрямовані на покращення життя усього людства, у протистоянні влади та злочинців, хакерів та поліції, ніхто не може бути впевненим у своїй безпеці.

З освоєннях просторів Інтернету, медицині довелося зустрітися з багатьма проблемами, такими як недостовірність інформації, різноманітні фальсифікації даних, атаки на БД лікарень. І ці спроби не завжди були невдалими.

Хакерські атаки, шпигунські дії, втручання у потоки інформації, все це стає актуальним для телемедицини. І для кожної з процедур, які вона може запропонувати, знайдеться нова загроза. Саме тому такими актуальними стають засоби захисту інформації, не тільки правові, як розробка нових законів та норм, сертифікація апаратних комплексів та програмних продуктів, а й засоби інформаційної безпеки, такі як антивірусні програми, файерволи, побудова безпечних корпоративних мереж VPN.

У даному напрямі проводиться багато досліджень кожного року, адже його актуальність розуміють усі. Проводяться дослідження конфіденційності та її збереження, доступності, фірми вибудовують власні політики безпеки та правила, які необхідно виконувати для забезпечення ІБ при використанні їх продукції. Проте комплексного підходу на даний момент не існує. Тому автор вважає за потрібне виконання дослідження загальної моделі. І перш за все, узагальнення підходу до забезпечення безпечного проведення телемедичних процедур.

З виділення основних напрямів атаки на кожну з процедур починається побудова моделі загроз. Окрім трьох основних властивостей інформації в контексті інформаційної безпеки, а саме конфіденційність, цілісність та доступність, у даному випадку слід також виділити деякі інші важливі компоненти телемедичних процедур.

1.4 Нормативна база телемедицини в Україні

На даний момент часу в Україні активно розвивається напрямок телемедицини, тому і законодавча база наздоганяє технології. Саме через ці перегони у працівників медичного закладу та у кінцевого споживача (людини) виникають сумніви щодо правильності роботи та захищеності їх «чутливої» інформації.

Одним із пріоритетних завдань розвитку телемедицини є вдосконалення нормативної бази, яке одночасно надзвичайно важливе для ефективного і якісного подальшого розвитку всієї системи охорони здоров'я України та її належного реформування. Необхідно розробити і затвердити законодавчі акти у сфері телемедицини й електронної охорони здоров'я, гармонізовані з юридичними нормами Європейського Союзу і методичними документами ВООЗ, нормативну доказову науково-методичну документацію, стандарти і протоколи, національну система електронних медичних записів, систему дистанційного навчання, електронного документообігу, інформаційні системи лікувально-профілактичних, освітніх і науково-дослідних установ, інформаційні фармацевтичні системи, системи захисту цифрової інформації.

Українська політична еліта не лише усвідомила важливість сучасної медицини, а й почала втілювати це розуміння в ключових політичних документах. Президентська програма реформ до 2020 р. та проект Коаліційної угоди проукраїнської більшості в парламенті називають реформу системи охорони здоров'я та, зокрема, розвиток телемедицини серед першочергових завдань.

Ще у 2007 р. було створено Державний клінічний науково-практичний центр телемедицини МОЗ України – єдиний спеціалізований заклад охорони здоров'я, створений для надання висококваліфікованої комплексної консультативної медичної допомоги населенню з застосуванням сучасних інформаційних та телемедичних технологій, організації заходів з розробки, апробації, впровадження їх та розвитку телемедицини в Україні.

За підтримки партнерів Центр телемедицини сьогодні реалізовує широкомасштабний проект «Телемедицина» в рамках Меморандуму, підписаного між МОЗ України, НАМНУ, компаніями ДТЕК, МТС, а також Благодійним фондом «Розвиток України», і є ключовим виконавцем і координатором зазначеного проекту, у якому задіяні медичні заклади і установи з 12 областей України. Цей проект спрямований на розвиток телемедицини в Україні шляхом інтеграції передового медичного досвіду та сучасних телекомунікаційних технологій.

З 2009 р. Центром телемедицини реалізується проект створення телемедичної мережі України, завдяки якій започатковано телемедичне консультування та обмін досвідом лікарів на Порталі телемедицини.

Телемедична мережа об'єднала МОЗ України, Державний клінічний науково-практичний центр телемедицини в Києві, Донецьку й Закарпатську обласні лікарні, Національний інститут серцево-судинної хірургії ім. М. М. Амосова НАМНУ, Інститут педіатрії акушерства та гінекології НАМНУ, Національний інститут хірургії та трансплантології ім. А. А. Шалімова НАМНУ, Інститут нейрохірургії ім. акад. А.П. Ромоданова НАМНУ, Національну дитячу спеціалізовану лікарню «ОХМАТДИТ», Львівську комунальну міську клінічну лікарню швидкої медичної допомоги, Львівську комунальну міську дитячу клінічну лікарню, Львівську обласну клінічну лікарню, Обласний державний онкологічний регіональний лікувально-діагностичний центр (перелік установ постійно оновлюється).

Галузевим нормативно-правовим документом для забезпечення упровадження телемедицини в охорону здоров'я є наказ МОЗ від 26.03.2010 р. № 261 «Про впровадження телемедицини в закладах охорони здоров'я».

ЇЇ нащадком став Законопроект «Про телемедицину» (№ 10196 від 14.03.2012 р.). Він визначав основні положення телемедицини, її призначення, фінансові та технологічні аспекти, та базувався на даних ВООЗ (Всесвітня організація охорони здоров'я). Проте він був відправлений на доопрацювання і наразі не підписаний.

Нові нормативні документи щодо застосування телемедицини у сфері охорони здоров'я затверджені Наказом МОЗ від 19.10.2015 № 681, зокрема:

1. Порядок організації медичної допомоги на первинному, вторинному (спеціалізованому), третинному (високоспеціалізованому) рівнях із застосуванням телемедицини (в тому числі вимоги до порталів телемедицини);
2. Положення про кабінет телемедицини закладу охорони здоров'я (в тому числі табель оснащення кабінету телемедицини);
3. Форми первинної облікової документації «Запит на телемедичне консультування», «Висновок консультанта», «Журнал обліку телемедичних консультацій» та інструкції щодо їх заповнення.

26 вересня 2016 р. Кабінет Міністрів України вніс зміни до «Переліку платних послуг, які надаються в державних закладах охорони здоров'я та вищих медичних закладах освіти». Згідно з рішенням уряду, закладам охорони здоров'я дозволяється надавати медичну допомогу із застосуванням телемедицини, що «забезпечить конституційне право громадян на якісну медичну допомогу і дозволить розширити доступ до таких послуг, а також буде сприяти ефективній організації надання медичної допомоги в умовах, коли відстань є критичним фактором» (постанова уряду № 648). Розширення переліку створить умови для залучення додаткових коштів юридичних і фізичних осіб за рахунок застосування телемедицини при наданні медичної допомоги як послуги, яка може бути надана пацієнту в будь-якому місці, де він її потребує, зазначається в постанові.

Кабмін включив у перелік ряд послуг, що надаються із застосуванням телемедицини. Зокрема, лабораторні, діагностичні та консультативні послуги за зверненням громадян, які надаються без направлення лікаря, у тому числі із застосуванням телемедицини, медична допомога хворим удома, у тому числі із застосуванням телемедицини (діагностичне обстеження, процедури, маніпуляції, консультації, догляд), медичне обслуговування, у тому числі із застосуванням

телемедицини, за договорами із суб'єктами господарювання, страховими організаціями, медичне обслуговування, у тому числі із застосуванням телемедицини, іноземних громадян.

Про активне впровадження системи телемедицини – медичної допомоги на відстані як в умовах повсякденного життя, так і в умовах надзвичайних ситуацій, у тому числі в умовах проведення антитерористичної операції – говорили учасники круглого столу «Розвиток національної системи телемедицини та парамедицини в Україні: впровадження міжнародних стандартів», організованого Комітетом ВР з питань охорони здоров'я (27 травня 2016 р.). [6]

1.5 Математичні методи оцінки та їх основні компоненти

Для оцінки ризиків використовуються кількісні та якісні методи оцінки. Математичне моделювання відноситься до групи кількісних методів. Якісні методи дозволяють дати комплексну оцінку вірогідності виникнення ризику і збитків від його реалізації, проте недоліком є те, що необхідно залучати компетентних експертів. Кількісні методи є в свою чергу більш трудомісткими, бпроте дозволяють визначити декілька альтернатив для прийняття рішення.

До кількісних методів відносяться наступні види:

1. Статистичний (регресивний аналіз, метод середніх величин і т.д.)
2. Логіко – ймовірнісний методи
3. Аналітичні методи
4. Методи аналогій

Статистичні методи кількісної оцінки найбільш часто використовуються для оцінки ризиків (регресійний аналіз, метод середніх величин і ін.). Дані методи засновані на розрахунку ймовірності настання випадкової події. Перевагою статистичних методів є простота розрахунків, недоліком - для достовірності необхідна наявність великої кількості ретроспективної інформації.

Логіко-імовірнісні методи застосовуються порівняно недавно. В економіці дана група методів використовується найчастіше в банківській сфері. За допомогою цих методів створені імовірнісна, логічна і структурна моделі кредитного ризику, а також обчислена ціна за ризик кредиту і міри ризику.

Метод аналогій, згідно з назвою, заснований на аналізі баз даних про оцінку ризиків об'єктів-аналогів. Обов'язковою умовою застосування даного методу є порівнянність інформації досліджуваного об'єкта з аналогічним. Цей метод зазвичай використовується для оцінки ризиків часто повторюваних подій або об'єктів.

Аналітична група методів частіше використовується для оцінки інвестиційних та інноваційних проектів і підрозділяється на дві підгрупи: методи без урахування розподілу ймовірності (стрес-тестування) і методи з урахуванням розподілу ймовірностей (нетрадиційні методи).

Математичні моделі і методи відносяться до аналітичної групи методів. Основна мета застосування математичного моделювання в оцінці ризиків зводиться до опису загальної моделі: $R = f(P, I)$, де P - ймовірність настання ризикової події, I - потенційні наслідки впливу факторів.

Використання математичних моделей в залежності від постановки задачі і наявності вихідної інформації можна звести до застосування таких типів моделей, як детерміновані, стохастичні, лінгвістичні і ігрові.

Ігрові (не стохастичні) моделі використовуються тоді і тільки тоді, коли відсутня вихідна інформація для використання інших типів моделей. На основі теорії ігор формуються кілька випадків при здійсненні ризику, і за допомогою статистичних та стратегічних ігор визначається значення заходи або ймовірності ризику.

Лінгвістичні моделі засновані на методах нечіткої логіки. Невизначеність описується функцією приналежності, завдяки якій не потрібно впевненість в повторюваності подій. Передбачається, що для використання даних методів є експертна оцінка про ступінь невизначеності.

Стохастичні моделі базуються на застосуванні статистичних розрахунків і наявності достатньої кількості статистичної інформації про будь-яку подію. За допомогою стохастичних моделей на заданій множині оцінюється ймовірність настання ризику, дані моделі застосовуються за умови випадковості виникнення факторів ризику.

За допомогою детермінованих моделей визначається найбільш достовірний результат, оскільки дані моделі застосовні в умовах, коли фактори виникнення ризику визначені і носять регулярний характер і наслідки прийнятих рішень призводять до певного результати. Для формування моделей використовуються інструменти математичного аналізу, логіки та ін. [7]

Висновки до розділу 1

У даному розділі був зроблений аналіз стану проблеми захисту інформації в телемедицині за першоджерелами.

Проаналізовано шість телемедичних процедур та класифіковано набір послуг, що надає кожна з них.

Проаналізовано нормативну базу телемедицини, яка існує на території України в даний момент часу.

Надано класифікацію методів оцінки уразливостей та математичних методів оцінки. Складності та необхідні дані для побудови кожної оцінки.

Розглянуто проблеми для проведення комплексної оцінки.

2 ПОПЕРЕДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ ОЦІНКИ

2.1 Виділення векторів

Для проведення повноцінної побудови моделі загроз необхідною складовою, на якій і побудована вся система, виступає платформа. Це комп'ютер, система, застосунок, програма чи будь-яка інша складова середовища, що буде досліджуватися. Для побудови моделі це ще і база даних, звідки будуть надходити необхідна інформація для оцінки уразливості та її вклад у побудову моделі інформаційної безпеки.

Оскільки у розділі першому було детально розглянуто та класифіковано кожен з видів телемедичних процедур, для остаточної класифікації необхідно визначити готові продукти, якими користується кожний з напрямків. Звісно що таких продуктів може бути велика кількість, тому розглянуто буде лише найпопулярніші. Зібравши статистику з відкритих джерел, автором буде вибрано від п'яти до десяти груп уразливостей, що є в більшості розглянутих платформ, які і буде досліджено для подальшої оцінки уразливостей.

Слід також враховувати, що навіть при великому бажанні не можна буде розглянути всі уразливості, не кажучи вже про всі такі проблеми для кожної з розглянутих платформ.

Тому буде зроблено вибірку, намагаючись знайти найбільш різноманітні загрози. Умовно кажучи, для побудови повноцінної моделі безпеки інформації, буде взято абстрактну платформу для кожної з телемедичних процедур, як і загальні випадки уразливостей (базуючись на вибірці уразливостей на більшості з практично використовуваних платформ). Саме це дозволить зробити найбільш повний аналіз для загального випадку та проведення подальших робіт в кожному з напрямків дослідження.

2.1.1 Телемедичне консультування

Для проведення телемедичного консультування згідно до програми розвитку телемедицини буде розроблено спеціалізовану платформу. На даному етапі стан цієї розробки невідомий, а єдиної оболонки для проведення консультування не існує. Зараз в Україні планується використовувати Skype та інші програми на зразок нього. І хоча в інших країнах існують свої програми для подібного зв'язку, з впевненістю можна сказати, що на даному етапі саме Скайп є яскравим прикладом використовуваної платформи. Також можна додати до цього різні продукти компанії TrueConf, створені для телеконференцій, що діють саме в Україні та Європі.

Окрім традиційного відео зв'язку також телемедичне консультування включає в себе документообіг. Коли лікар та пацієнт можуть спілкуватися між собою за допомогою форумів, листів.

Уразливості:

1. Механізм генерації одноразових кодів для відновлення паролю.
2. Уразливість тех. підтримки.
3. Можливість прихованих сесій.
4. Уразливість розкриття IP-адреси.
5. Відсутність точної інформації щодо причин блокування/додаткової перевірки.
6. Можливість завантаження додаткового софту.
7. Відсутність підтвердження сторін при встановленні сесії.
8. Вразливість каналу передачі даних.
9. Можливість встановлення людини-по-середині.
10. Несумісність чи особливість налаштувань систем ПЗ.

2.1.2 Біотелеметрія (телемоніторинг)

Системи біотелеметрії та телемоніторингу включають в себе не тільки програмну частину, як було з телеконсультуванням, але і апаратний багаж. Не дивлячись на те, що системи є досить новими, у світі вже є декілька великих корпорацій, що зосередилися саме на виробництві платформ цього типу. Сюди входять не тільки системи лікарень, що підтримують життя в тяжкохворих та безперервно передають інформацію на пост медсестрі, але і кардіостимулятори, обладнання діагностування що майже все зараз передає данні на екрани лікарів.

Виробники Medtronic, Nanostim, General Electric Healthcare.

Таке обладнання потребує великих коштів та точності, саме тому майже кожен сезон товари на ринку змінюються, лінійки та індивідуальні вироби не дозволяють з впевненістю назвати марки виробів, проте виробники, які впевнено зайняли свої ніші, вже є.

Уразливості:

1. Електромагнітне випромінювання середовища (ненавмисне).
2. Пошкодження каналу передачі даних.
3. Помилка апаратури.
4. Фізичний вплив.
5. Відсутність автентифікації.

2.1.3 Домашня (індивідуальна) телемедицина

Домашня телемедицина є досить популярним напрямом, що росте з кожним днем. Не тільки за кількістю користувачів, але і за кількістю різноманітних платформ. Вона вміщує в собі як телемедичне консультування, так и біотелемедицину. Тому загрози для цього напряму процедур тут можуть повторюватися. Але їх пріоритетність трохи інша.

Також при користуванні домашньою телемедициною пацієнт підпадає і під дію уразливостей браузера, що використовується. Окрім Скайпа, Опери, Хрома та декількох інших представників, поруч з ними конкурують дорогі комплекси підтримання життєзабезпечення та системи Розумний будинок.

Уразливості:

1. Відсутність підтвердження повноти, достовірності та компетентності автора інформації.
2. Уразливість паролів користувача.
3. Уразливість браузера користувача (шкідливе ПО, XSS).
4. Втручання в канал.
5. Можлива втрата конфіденційної інформації (виток).
6. Крадіжка особистості.
7. Уразливість служби технічної підтримки.

2.1.4 Телескринінг

Складний комплекс програм та апаратури, що призначено для великих обсягів даних. Хоча обладнання і є дорогим, через свої попереджувальні заходи ця процедура є досить популярною.

Уразливості:

1. Уразливість коду ПЗ.
2. Фізичне втручання.
3. Помилка програмування.
4. Несумісність ПЗ на різних видах обладнання.
5. Відсутність автентифікації сторін.
6. Уразливість каналу передачі даних.
7. Порушення структури БД.

2.1.5 Телеприсутність/телеасистування

Дорогий не тільки комплекс, але і час, що використовується при проведенні такого роду процедур. Вони дозволяють молодим лікарям навчатися у визнаних геніїв своєї справи, біти присутніми на найрізноманітніших конференціях, операціях та семінарах. Спеціалісти навчаються не тільки у майстрів, але і можуть допомогти при проведенні операції.

Окрім цього, сам лікар може проводити операцію, знаходячись у зовсім іншій точці планети. І, звісно, така технологія є не просто дорогою на даний момент часу, але і досить унікальною.

Medtronic, MEYTEC GmbH Medizinsysteme є одними з лідерів у гонці за методикою телехірургії. Звісно, таких компаній ще не мало, а саме обладнання для проведення таких операцій поки що не виходить великим тиражем, проте і великої статистики загроз для них не існує. Однак перші спроби з обох боків вже були, хоча і поодинокі.

Уразливості:

1. Втручання в канал (навмисне).
2. Крадіжка інформації.
3. Відсутність суворого контролю доступу до телеконференції при проведенні процедур.
4. Помилка апаратури, ПЗ.
5. Вплив середовища (випадкове).
6. Фізичний вплив на апаратуру.

2.1.6 Дистанційне навчання

Дистанційне навчання є одним з найпопулярніших видів проводження часу в Інтернеті. І це стосується не лише телемедицини, але й інших напрямів. Було створено безліч спеціалізованих сайтів, тисячі блогів та платформ, що дозволяють

користувачам отримувати інформацію напряму від лікарів. Перш за все, навіть звичайний браузер може бути частиною системи дистанційного навчання. Тому усі його вразливості стають уразливостями користувачів. Саме тому це є одним з найбагатших для зловмисників угідь [8].

Уразливості:

1. XSS (Cross-Site Scripting).
2. SQL Injection.
3. Information Leakage.
4. Brute force та інші махінації з паролями.
5. XML External Entities (впровадження зовнішніх сутностей XML).
6. Path Traversal (обхід шляху).
7. DoS (Denial Of Service).
8. Unvalidated Redirects and Forwards (відкриті редіректи).
9. Broken Authentication and Session Management.
10. Insecure Direct Object References (незахищені ресурси та об'єкти).

2.2 Пріорітизація загроз для телемедицини на основі CVSS

Існують різноманітні способи та методи для проведення оцінки стану захищеності системи та виявлення уразливостей у ній. Використовуючи виділені вектори та дані, що було отримано у попередні роботі[8], наразі ми можемо використати їх у вигляді табличних даних і не розписувати виникнення кожного з чисел. У подальшому ці дані знадобляться для оцінювання результатів на основі різних моделей.

На сьогоднішній день найбільш широке практичне застосування знайшли наступні способи класифікації та кількісної оцінки актуальності уразливостей: схема класифікації уразливостей NIPC, шкала аналізу уразливостей SANS, система оцінки критичності уразливостей Microsoft, система оцінки уразливостей за стандартом PCI DSS, системи US—CERT, CVSS та nCircle. Вони відрізняються

врахованими при класифікації уразливостей параметрами та шкалами оцінки уразливостей[6].

Найбільш простим у використанні є CVSS, що є доступним для широкого загалу в безкоштовному вигляді в Інтернеті з докладною інструкцією. Цей інструментарій дозволить провести оцінку критичності уразливості, не маючи великого практичного досвіду в даній сфері, а для спеціалістів дозволить налаштувати гнучкі вхідні дані, щоб з версії 3.0 оцінити не тільки критичність ізольованої уразливості, а її подальшу динаміку. Тобто даний інструментарій дозволяє проводити дослідження не лише самої уразливості, але і можливі наслідки її реалізації в контексті середовища.

На даний час доступно дві версії програми, а саме CVSSv2 та CVSSv3. Відповідно, саме цей інструментарій буде розглянуто, а також наведено обґрунтування для використання останньої версії програми.

2.2.1 Загальне визначення системи CVSS

CVSS пропонує простий інструмент для розрахунку чисельного показника по десятибальній шкалі, який дозволяє оперативно приймати рішення щодо того, як реагувати на ту чи іншу уразливість. Чим вище значення метрики, тим оперативніші дії мають бути проведені. [9]

До стандарту входять три групи метрик:

1. Базові метрики описують характеристики уразливостей, що не змінюються з плином часу та не залежать від навколишнього оточення. Ці метрики описують складність експлуатації уразливості та потенційний збиток для конфіденційності, цілісності та доступності інформації.
2. Часові метрики вносять загальну в загальну оцінку правку на повноту наявної інформації про уразливість, зрілість експлуатаційного коду (якщо він є) та доступність виправлень.

3. Контекстні метрики вносять до загальної оцінки правки щодо характеристик інформаційного середовища.

Часові та контекстні метрики опціональні та використовуються для більш точної оцінки загрози, яку становить дана уразливість для більш чи менш конкретної інфраструктури.

В рамках стандарту було введено такі поняття:

- уразливий компонент (vulnerable component) – той компонент інформаційної системи, який містить уразливість та схильний до експлуатації;
- атакований компонент (impacted component) – той, конфіденційність, цілісність та доступність котрого можуть постраждати в разі вдалої реалізації атаки.

У більшості випадків уразливий та атакований компоненти співпадають, проте є цілі класи уразливостей, для яких це не так, наприклад:

- вихід за межі пісочниці застосунку;
- отримання доступу до користувацьких даних, збережених в браузері, через уразливість у веб-застосунках (XSS);
- вихід за межі гостьової віртуальної машини.

Згідно до нового стандарту, метрики експлуатування розраховуються для уразливого компонента, а метрики впливу для атакованого. В CVSSv2 не було можливості описати ситуацію, коли уразливий та атакований компоненти відрізняються.

2.2.2 Шкали в метриках, умовні позначення

Вектор доступу. Коли уразливість може експлуатуватися і локально, і через мережу, вибирається значення "Network". Коли уразливість може експлуатуватися локально і з суміжних мереж, але не з видалених мереж, вибирається значення

"Adjacent Network". Коли уразливість може експлуатуватися з суміжних і віддалених мереж, то вибирається значення "Network". В третій версії було розділено локальний доступ на локальний та фізичний, що показано в Таблиці 2.1

Таблиця 2.1 – Вектор доступу та його можливі значення

CVSSv2	CVSSv3
Назва метрики	
Access Vector (AV)	Attack Vector (AV)
Можливі значення метрики	
Network (N)	Network (N)
Adjacent Network (A)	Adjacent Network (A)
Local (L)	Local (L)
	Physical (P)

Складність експлуатації уразливості. Якісна оцінка складності проведення атаки. Чим більше умов має бути дотримане для експлуатації уразливості — тим вище складність. Можливі значення метрики показані в Таблиці 2.2.

Таблиця 2.2 – Складність експлуатації уразливості та її можливі значення

CVSSv2	CVSSv3
Назва метрики	
Access Complexity (AC)	Attack Complexity (AC)
Можливі значення метрики	
Low (L)	Low (L)
Medium (M)	
High (H)	High (H)

Аутентифікація/необхідний рівень привілегій. Чи потребує проведення атаки аутентифікації, якщо так, то якої. Якщо уразливість існує в схемі аутентифікації (наприклад, PAM, Kerberos) або в анонімному сервісі (наприклад, загальнодоступний ftp-сервер), метрика вибирається як "None", оскільки

зловмисник може експлуатувати уразливість, якщо не надасть дійсні облікові дані. Існування стандартного облікового запису описується як "Single" або "Multiple" Authentication (залежно від ситуації), але Exploitability може бути "High", якщо облікові дані розголошені. Можливі значення метрики показані в Таблиці 2.3.

Таблиця 2.3 – Необхідний рівень привілегій та його можливі значення

CVSSv2	CVSSv3
Назва метрики	
Authentication (Au)	Privileges Required (PR)
Можливе значення метрики	
Multiple (M)	
Single (S)	
	High (H)
	Low (L)
None (N)	None (N)

Необхідність взаємодії з користувачем. Чи потрібні для успішної реалізації атаки які-небудь дії з боку користувача системи, що атакується. Можливі значення метрики показані в таблиці 2.4.

Таблиця 2.4 – Необхідність взаємодії з користувачем

CVSSv2	CVSSv3
Назва метрики	
	User Interaction (UI)
Можливі значення метрики	
	None (N)
	Required (R)

Границі експлуатації. Чи відрізняються експлуатовані та атаковані компоненти, тобто чи дозволяє експлуатація уразливості порушити конфіденційність, цілісність і доступність якого-небудь іншого компонента системи. В Таблиці 2.5 показані можливі значення метрики.

Таблиця 2.5 – Границі експлуатації та її можливі значення

CVSSv2	CVSSv3
Назва метрики	
	Scope (S)
Можливі значення метрики	
	Unchanged (U)
	Changed (C)

Метрики впливу. Оцінка міри впливу на конфіденційність, цілісність і доступність компонента, що атакується. В Таблиці 2.6 показані можливі значення.

Таблиця 2.6 – Метрики впливу та їх можливі значення

CVSSv2	CVSSv3
Назва метрики	
Confidentiality Impact (C), Integrity Impact (I), Availability Impact (A)	
Можливі значення метрики	
None (N)	None (N)
Partial (P)	
Complete (C)	
	Medium (M)
	High (H)

Ступінь зрілості доступних засобів експлуатації. Чи доступний публічно код або інші засоби, за допомогою яких можна провести атаку, або існує лише теоретична можливість експлуатації. Можливі значення подано в Таблиці 2.7

Таблиця 2.7 – Ступінь зрілості доступних засобів експлуатації

CVSSv2	CVSSv3
Назва метрики	
Exploitability (E)	Exploit Code Maturity (E)
Можливі значення метрики	
Not Defined (ND/X)	
High (H)	
Functional (F)	
Proof-of-Concept (POC/P)	
Unproven (U)	

Доступні засоби усунення уразливостей. Чи існують офіційні або неофіційні засоби усунення уразливості. Можливі значення метрики наведені в Таблиці 2.8.

Таблиці 2.8 – Доступні засоби усунення уразливостей

CVSSv2	CVSSv3
Назва метрики	
Remediation Level (RL)	
Можливі значення метрики	
Not Defined (ND/X)	
Unavailable (U)	
Workaround (W)	
Temporary Fix (TF/T)	
Official Fix (OF/O)	

Ступінь довіри до інформації про уразливість. Міра деталізації доступних звітів про уразливість. Дані подано в Таблиці 2.9

Таблиця 2.9 – Ступінь довіри до інформації про уразливість

CVSSv2	CVSSv3
Назва метрики	
Report Confidence (RC)	
Можливі значення метрики	
Not Defined (ND)	Not Defined (X)
Unconfirmed (UC)	
Uncorroborated (UR)	
	Unknown (U)
	Reasonable (R)
Confirmed (C)	Confirmed (C)

Якісна шкала оцінки небезпеки. За роки використання CVSSv2 в різних компаніях склалися різні підходи до виставляння якісного рівня небезпеки на базі метрики CVSS:

- Nvd.nist.gov: 0—3.9 Low; 4.0—6.9 Medium; 7.0—10.0 High;
- Tenable: 0—3.9 Low; 4.0—6.9 Medium; 7.0—9.9 High; 10.0 Critical;
- Rapid 7: 0—3.9 Moderate; 4.0—7.9 Severe; 8.0—10.0 Critical.

2.2.3 Особливості формул для обрахунку

Базова формула. Базова формула – це основа обчислення CVSS.

Часова формула. При використанні часової формули часові метрики об'єднуються з базовими, щоб вивести часову оцінку в інтервалі від 0 до 10. Часова оцінка не перевищує базову і не більше ніж на 33% менше її.

Контекстна формула. При використанні контекстних формул контекстні метрики об'єднуються з часовими метриками, щоб отримати оцінку оточення в інтервалі від 0 до 10. Значення контекстної метрики, отримане з цієї формули, не повинне перевищувати тимчасову оцінку.

2.2.4 Телемедичне консультування

Виходячи з Розділу 2.1, телемедичне консультування має десять типових груп уразливостей. Спочатку буде наведено дані на вхід, в кінці кожного з підпунктів до Таблиці 2.10 винесено оцінки, отримані в результаті обробки вхідних даних за допомогою програмної оболонки CVSSv3.0.

Таблиця 2.10 – Оцінки уразливості в телемедичному консультуванні

Уразливість	Базова метрика	Часова метрика	Контекстна метрика	Висновок
1	2	3	4	5
1. Механізм генерації одноразових кодів для відновлення паролю	9.3	9.3	9.3	Критична
2. Уразливість тех. підтримки	6.1	5.6	5.0	Середня

Продовження таблиці 2.10

1	2	3	4	5
3. Можливість прихованих сесій	5.8	5.4	5.4	Середня
4. Уразливість розкриття IP-адреси	6.1	5.5	5.5	Середня
5.Відсутність точної інформації щодо причин блокування/додаткової перевірки	9.9	9.9	9.9	Критична
6. Можливість завантаженні додаткового софту	7.3	7.1	7.1	Висока
7. Відсутність підтвердження сторін при встановленні сесій	6.1	6.0	6.0	Середня
8. Вразливість каналу передачі даних	8.9	8.7	8.7	Висока
9. Можливість встановлення людини-по-середині	6.1	6.0	6.0	Середня
10. Несумісність чи особливість налаштувань систем ПЗ	6.3	6.2	6.2	Середня

2.2.5 Біотелеметрія (телемоніторинг)

Виходячи з Розділу 2.1, телемоніторинг має п’ять типових груп уразливостей. Спочатку буде наведено дані на вхід, в кінці кожного з підпунктів до Таблиці 2.11 винесено оцінки, отримані в результаті обробки вхідних даних за допомогою програмної оболонки CVSSv3.0.

Таблиця 2.11 – Оцінки уразливості в біотелеметрії

Уразливість	Базова метрика	Часова метрика	Контекстна метрика	Висновок
1. Електромагнітне випромінювання середовища (ненавмисне)	7.8	7.3	7.3	Висока
2. Пошкодження каналу передачі даних	6.5	6.1	6.1	Середня
3. Помилка апаратури	6.8	6.4	6.4	Середня
4. Фізичний вплив	6.7	6.3	6.3	Середня
5.Відсутність автентифікації	6.5	6.1	6.1	Середня

2.2.6 Домашня (індивідуальна) телемедицина

Виходячи з Розділу 2.1, домашня телемедицина має сім типових груп уразливостей. Спочатку буде наведено дані на вхід, в кінці кожного з підпунктів до Таблиці 2.12 винесено оцінки, отримані в результаті обробки вхідних даних за допомогою програмної оболонки CVSSv3.0.

Таблиця 2.12 – Оцінки уразливості в індивідуальній телемедицині

Уразливість	Базова метрика	Часова метрика	Контекстна метрика	Висновок
1. Відсутність підтвердження повноти/достовірності інформації та компетентності автора інформації	6.8	6.5	6.5	Середня
2. Уразливість паролів користувача	8.8	8.4	8.4	Висока
3. Уразливість браузера користувача (шкідливе ПО, XSS)	8.3	7.9	7.9	Висока
4. Втручання в канал	6.5	6.2	6.2	Середня
5.Можлива втрата конфіденційної інформації (виток)	6.9	6.6	6.6	Середня
6. Крадіжка особистості	7.7	7.4	7.4	Висока
7. Уразливість служби технічної підтримки	7.1	6.8	6.8	Середня

2.2.7 Телескринінг

Виходячи з Розділу 2.1, телескринінг має сім типових груп уразливостей. Спочатку буде наведено дані на вхід, в кінці кожного з підпунктів до Таблиці 2.13 винесено оцінки, отримані в результаті обробки вхідних даних за допомогою програмної оболонки CVSSv3.0.

Таблиця 2.13 – Оцінки уразливостей в телескринінгу

Уразливість	Базова метрика	Часова метрика	Контекстна метрика	Висновок
1. Уразливість коду ПЗ	2.8	2.6	2.6	Низька
2. Фізичне втручання	6.5	6.0	6.0	Середня
3. Помилка програмування	6.9	6.4	6.4	Середня
4. Несумісність ПЗ на різних видах обладнання	6.5	6.0	6.0	Середня
5.Відсутність автентифікації сторін	7.5	7.0	7.0	Висока
6. Уразливість каналу передачі даних	6.8	6.3	6.3	Середня
7. Порушення структури БД	6.8	6.3	6.3	Середня

2.2.8 Телеприсутність/телеасистування

Виходячи з Розділу 2.1, телеприсутність має шість типових груп уразливостей. Спочатку буде наведено дані на вхід, в кінці кожного з підпунктів до Таблиці 2.14 винесено оцінки, отримані в результаті обробки вхідних даних за допомогою програмної оболонки CVSSv3.0.

Таблиця 2.14 – Оцінки уразливості в телеприсутності/телеасистуванні

Уразливість	Базова метрика	Часова метрика	Контекстна метрика	Висновок
1. Втручання в канал (навмисне)	7.9	7.5	7.5	Висока
2. Крадіжка інформації	5.8	5.8	5.8	Середня
3. Відсутність контролю доступу до телеконференції при проведенні процедур	6.5	6.2	6.2	Середня
4. Помилка апаратури, ПЗ	6.6	6.3	6.3	Середня
5.Вплив середовища (випадкове)	5.3	5.0	5.0	Середня
6. Фізичний вплив на апаратуру	6.9	6.5	6.5	Середня

2.2.9 Дистанційне навчання

Виходячи з Розділу 2.1, дистанційне навчання має десять типових груп уразливостей. Спочатку буде наведено дані на вхід, в кінці кожного з підпунктів до Таблиці 2.15 винесено оцінки, отримані в результаті обробки вхідних даних за допомогою програмної оболонки CVSSv3.0.

Таблиця 2.15 – Оцінки уразливості в дистанційній телемедицині

Уразливість	Базова метрика	Часова метрика	Контекстна метрика	Висновок
1	2	3	4	5
1. XSS (Cross-Site Scripting)	8.8	8.4	8.4	Висока
2. SQL Injection	8.3	7.9	7.9	Висока
3. Information Leakage	7.1	6.9	6.9	Середня
4. Brute force та інші махінації з паролями	8.3	7.9	7.9	Висока
5. XML External Entities (впровадження зовнішніх сутностей XML)	8.3	7.9	7.9	Висока
6. Path Traversal (обхід шляху)	7.4	7.1	7.1	Висока
7. DoS (Denial Of Service)	10.0	9.5	9.5	Критична
8. Unvalidated Redirects and Forwards (відкриті редіректи)	5.4	5.2	5.2	Середня

Продовження таблиці 2.15

1	2	3	4	5
9. Broken Authentication and Session Management	7.7	7.4	7.4	Висока
10. Insecure Direct Object References (незахищені ресурси та об’єкти)	7.1	6.8	6.8	Середня

Висновки до розділу 2

У цьому розділі було проаналізовано теоретичні дані з Розділу 1 та зроблено відбірку груп уразливостей.

Було проаналізовано методи для подальшої обробки даних. Наведено дані, що отримано у попередній роботі[8] та систематизовано їх в таблицю. Вибрано та описано ті вектори, які дозволять обчислити оцінку уразливості найбільш доцільно виходячи з логічних міркувань.

Таким чином даний розділ дав нам вся необхідні статистичні та практичні дані для подальшої побудов і обрахунків математичних оцінок.

3 ПОБУДОВА МАТЕМАТИЧНИХ МОДЕЛЕЙ ОЦІНКИ

Слід зазначити, що на даний момент часу не існує єдиної системи та уніфікованого способу, які б дозволили провести оцінку системи та її уразливостей. А для оцінки ризику є декілька невід'ємних складових.

Перш за все, ризик в контексті інформаційної безпеки: ризик, пов'язаний з використанням інформаційних систем, які підтримують місію та бізнес-функції організації. З точки зору інформаційної безпеки ризик розглядають як добуток втрат від порушення конфіденційності, цілісності, автентичності або доступності інформаційних ресурсів на імовірність такого порушення. Ризики інформаційної безпеки розглядають як частину бізнес-ризиків та обробляють схожим чином.

Будь-яке оцінювання ризиків інформаційної безпеки починається з обстеження інформаційної системи, ідентифікації інформаційних ресурсів та опису технологій обробки інформації.

Ризики інформаційної безпеки класифікуються за:

1. Властивостями інформаційних ресурсів, які порушуються при реалізації ризику (конфіденційність, цілісність, доступність, автентичність, спостережність);
2. Видимістю втрат внаслідок реалізації ризиків.

Можливі види втрат з результатами реалізації ризиків:

1. фінансові втрати;
2. репутаційні втрати;
3. порушення законодавства/контрактів;
4. шкода продуктивності персоналу;
5. загроза життю і здоров'ю людей.

З наведених вище видів втрат більш-менш точно можуть бути оцінені фінансові втрати. З меншою точністю у грошовому вимірі можуть бути оцінені втрати від шкоди продуктивності персоналу та порушення законодавства/контрактів, тому що реалізація певних ризиків може тягнути не

тільки фінансові санкції (штрафи, цивільні позови), але і санкції, які не можуть бути оцінені фінансово (позбавлення ліцензії, кримінальна відповідальність тощо). Репутаційні втрати та загроза життю і здоров'ю людей не можуть бути оцінені фінансово.

Імовірність реалізації ризиків також часто не може бути оцінена точно. Джерелами відомостей щодо імовірності реалізації ризиків можуть бути дані про аналогічні випадки від державних органів, команд реагування на комп'ютерні надзвичайні події, галузевих асоціацій. Однак усі ці дані є, як правило, неповними (не всі компанії підлягають моніторингу), неточними (багато компаній не розкривають подробиці інцидентів інформаційної безпеки) і неактуальними (наприклад на початку хвилі чергового вірусу у зазначених даних відомості про вірус ще відсутні). Крім того, ці дані не враховують специфіку конкретного бізнесу. Тому статистичні дані про інциденти інформаційної безпеки, які вже відбулись, при оцінці ризиків приймаються до відома, але застосовуються із обережністю.

Внаслідок того, що ні втрати, ні імовірність не можуть бути оцінені чисельно, значення ризику не може бути обчислене відповідно до визначення. Замість цього використовують методи оцінки ризиків, які ґрунтуються на якісних показниках [9].

Для обчислення ймовірностей настання того чи іншого ризику, а також їх впливу на кінцевого споживача, слід дослідити ризик як складний процес, що поєднує в собі декілька складових частин.

На думку автора таке дослідження, яке зазвичай виконують соціальні працівники та працівники у сфері забезпечення охорони здоров’я, необхідне і тут. Причин тому декілька і найголовніша з них: сама телемедицина. Це не просто звичайна компанія, а структура, що відповідає за життя людей. І для неї важливими складовими є не тільки вразливості, загрози та спроби їх перекриття в значенні інформаційної безпеки, але ї середовище, місцезнаходження обладнання, системи передач данних між споживачем та телемедичним обладнанням.

На Рисунку 3.1 показано складові частини ризиків в телемедицині з урахування особливостей територій та технологій на території України.

Рисунок 3.1 – Складові частини ризику в телемедицині

3.1 Складові частини моделі

На Рисунку 3.1 зображено складові частини ризику, які буде розглянуто. Це основне зображення, складові, на яких будується оцінка ризику. І перш за все, слід визначитися, де у даній моделі використовується математична модель оцінки ризиків і які з семи складових вона охоплює.

Технічний ризик — ймовірність відмови технічних пристроїв з наслідками певного рівня (класу) за певний період функціонування небезпечного виробничого об'єкта [10]. Для телемедицини це безумовно обладнання. При проведенні рентгену, МРТ та інших процедур, можуть бути виділені шкідливі відходи та завдано збитку життю людини (кінцевого споживача).

Індивідуальний ризик — частота ураження окремої людини в результаті впливу досліджуваних факторів. Це не тільки ризики, які існують для кінцевого

споживача, але й ризики для персоналу. А також сюди слід віднести складову частину оприлюднення «чутливої» інформації.

Потенційний територіальний ризик (або потенційний ризик) — частота реалізації вражаючих факторів аварії в розглянутій точці території. Окремим випадком територіального ризику є екологічний ризик, який виражає ймовірність екологічного лиха, катастрофи, порушення подальшого нормального функціонування та існування екологічних систем та об'єктів в результаті антропогенного втручання в природне середовище або стихійного лиха[9]. Для телемедичних процедур це не тільки місце, де знаходиться кінцевий споживач, проте і середовище, де функціонує обладнання.

Колективний ризик (груповий, соціальний) — це ризик прояву небезпеки того чи іншого виду для колективу, групи людей, для певної соціальної чи професійної групи людей. Окремим випадком соціального ризику є економічний ризик, який визначається співвідношенням користі і шкоди одержуваного суспільством від розглянутого виду діяльності[10]. Для телемедицини це не тільки ризик людей, але й репутаційний ризик для медицини в загалом. Оскільки телемедицина направлена в першу чергу на порятунок життя людей, яким неможливо надати допомогу в звичайній ситуації, цей пункт несе в собі загрозу як персоналу, так і життю кінцевого споживача.

Прийнятний (допустимий) ризик аварії — ризик, рівень якого допустимо і обґрунтований виходячи з соціально-економічних міркувань. Ризик експлуатації об'єкта є прийнятним, якщо заради вигоди, одержуваної від експлуатації об'єкта, суспільство готове піти на цей ризик. Таким чином, прийнятний ризик являє собою деякий компроміс між рівнем безпеки і можливостями його досягнення. Величина прийнятного ризику для різних суспільств, соціальних груп і окремих людей — різна. Наприклад, для Європейців і Індусів, жінок і чоловіків, багатих і бідних. В даний час прийнято вважати, що для дії техногенних небезпек в цілому індивідуальний ризик вважається прийнятним, якщо його величина не перевищує 10^{-6}[9]. Для телемедицини це також є справедливим, оскільки не кожна людина

погодиться проходити лікування на діагностику, тут має місце репутаційний ризик та саме в цьому пункту найбільшу роль буде відігравати побудова моделей та наглядна оцінка, оскільки саме тут кінцевий споживач має вирішувати, буде він проходити телепроцедуру чи ні.

Професійний ризик — це ризик, пов'язаний з професійною діяльністю людини[10]. Це ризик для рятувальників, ризики для лікарів, які обслуговують небезпечне обладнання та працюють у середовищі, де може виникнути загроза.

Інформаційний ризик – це ризик, пов’язаний з інформаційною оболонкою телемедицини. Не тільки репутаційна складова, що базується на людській думці, проте і частина інформації, що циркулює в системі. І сама технологія телепроцедур як така.

Тобто, деякі складові такого розгалуження ризиків перекривають один одного для більш комфортного і наглядного дослідження. І виокремити ми можемо декілька складових, які в загальному випадку будуть складами повну картину для розуміння ризику.

Першою такою складовою буде репутаційна на інформаційна складові. Для телемедицини це є чи не найважливою частиною. І в ній застосування математичних моделей і побудов також є чи не найбільш комфортним способом.

Другою важливою складовою є безпосередньо складова інформаційної безпеки. Сюди ж можна віднести складову частину обладнання та каналів зв’язку.

Окрема складова це середовище. Не як середовище функціонування, проте як середовище життєдіяльності системи. Це природні і техногенні фактири, що будуть впливати на телемедицину на території України.

3.2 Інформаційна складова

Виходячи з попередньої роботи[11], ми отримали усі необхідна нам дані для дослідження цього пункту. Тут ми повинні враховувати, що для найкращого результату необхідно не просто оприлюднити інформацію та дані, що було

отримано, проте й активно їх просувати. Чим більше споживачів будуть усвідомлювати небезпеки, та дії, що напрямлені на зниженні загроз, тим більше буде рівень довіри до телемедичних процедур та телемедицини в цілому.

І тут слід враховувати, що це не є боротьбою за споживача поміж декількох фірм чи приватних клінік, проте є боротьбою спільною за краще майбутнє та порятунок життів.

3.2.1 Оцінка ймовірностей за CVSS

У Таблиці 3.1 представлено дані з використання програмної оболонки CVSSv3.0 [9] та методу проведення експертних оцінок Делфі. Цей метод було використано для двох раундів, для кращих результатів та експертних значень.

Таблиця 3.1 – Джерела інформації в телемедичних процедурах

Телемедичні процедури	Люди		Програми		Програмно-апаратні комплекси	
	Кількість уразливостей	Середня оцінка	Кількість уразливостей	Середня оцінка	Кількість уразливостей	Середня оцінка
Телемедичне консультування	3	6.97	5	6.66	2	7.45
Біотелеметрія (телемоніторинг)	-	-	1	6.1	4	6.53
Домашня (індивідуальна) телемедицина	4	7.28	2	7.25	1	6.2
Телескринінг	-	-	5	5.66	2	6.15
Телеприсутність/телеасистування	2	6.0	2	6.9	2	5.75
Дистанційне навчання	1	7.9	9	7.46	-	-
Загальні дані:	10	7.04	24	6.67	11	6.42

Таблиця 3.1 показує нам загальні дані по вектору уразливості, базуючись на джерелі інформації, для якого можлива реалізація уразливості. Це єдиний показник, який не було детально розписано в оцінці уразливості, та, виходячи з якого, навіть людина без особливого досвіду у сфері інформаційної безпеки може побачити тенденцію та підготуватися.

Колонки таблиці описують наступні дані:

- телемедичні процедури – список процедур, які було детально розглянуто в Розділі 1;
- джерело інформації «люди» - де головним фактором виступає саме людський фактор;
- джерело інформації «програми» - де головним носієм інформації та фактором виступає програмна оболонка, ПЗ;
- джерело інформації «програмно-апаратний комплекс» - де головним носієм інформації виступає не тільки ПЗ, а й обладнання, для якого воно реалізовано, спеціалізовані комплекси та технічні засоби, що є невід'ємною частиною системи;
- кількість уразливостей – чисельне значення груп уразливостей, що можуть бути реалізовані для кожного конкретного джерела інформації, базуючись на розглянутому у підпунктах 1 та 2 Розділу 2 описі кожної конкретної уразливості у значенні оцінки уразливості;
- середня оцінка – середнє арифметичне значення оцінок уразливостей, що підпадають під відповідну категорію для джерел інформації;
- загальні дані – загальна кількість уразливостей та середня арифметична оцінка для кожного джерела інформації.

3.2.2 Оцінка ризику інформаційної складової

Для проведення подальшої оцінки буде використано бальну шкалу та підхід до оцінки ризику спираючись на ризик-утворюючий фактор.

У нас є ситуація, де замість можливих збитків існує невизначеність. Вірогідності визначені за допомогою експертної оцінки, тому і для того, щоб обрахувати загальну систему, використано експертний метод.

Представлено формулу:

$$R = \sum_{i=1}^{i} p_i * q_i$$

У ній є два показники, першим є показник ймовірності. Він визначає вірогідність того, що саме ця подія трапилася. Тут розуміється, що не використано вірогідність виникнення ситуації, а вже трапилася подія. І її характер буде визначено за одним з трьох показників – джерел інформації, оскільки збитки, які вони можуть нанести системі, є різними. Другий показник дає бальну оцінку для характеру збитків і виражає лінгвістичну змінну, визначну експертами для встановлення можливих збитків від тієї чи іншої події. У Таблиці 3.1 ці дані представлено як Середні оцінки. Це бальна шкала, визначена експертами та системою, яка виражається в контексті CVSS як міра небезпеки, а у формулі як бальна шкала від 1 до 10-ти, яка характеризую цю загрозу як збиток, який вона принесла своєю реалізацією.

Таким чином, можна оцінити, яким буде ризик для кінцевого споживача, який використовую ту чи іншу телепроцедуру.

В Таблиці 3.2 представлено результати обрахунку та оцінки.

Таблиця 3.2 – Бальна оцінка ризику

Телемедичні процедури	*Оцінка ризику*
Телемедичне консультування	6.911
Біотелеметрія (телемоніторинг)	6.444
Домашня (індивідуальна) телемедицина	7.117
Телескринінг	5.8
Телеприсутність/телеасистування	6.21
Дистанційне навчання	7.504

3.3 Особливості середовища функціонування.

Хоча в контексті інформаційної безпеки екологічні та техногенні фактори не є тим, що розглядається, проте для кібербезпеки це є важливим. І неможливо пройти повз, коли розглядається залежність апаратури та майбутній розвиток телемедицини, коли ми говоримо про просування та подальше функціонування телемедицини на території України.

Однією зі складових частин моделювання та прогнозування є обробка інформації, зібраної на основі спостережень за схожими ситуаціями. Цей метод дозволяє уникнути неточності щодо експертних даних та спиратися виключно на фактичні дані при побудові моделі.

Для розвитку якогось процесу і явища неможливо будувати виключно «парникові» умови, слід враховувати, що можуть і будуть траплятися неприємності. Однією з таких неприємностей є НС. Надзвичайні ситуації це невід'ємна складова умов існування людини, адже де є система, там є і порушення її цілісності.

НС не являються прямою загрозою для інформаційної системи, окрім випадків, коли несуть побічні збитки, проте в контексті кібербезпеки та телемедицини ситуація різко змінюється. Якщо вважати інформаційну безпеку як систему, що залежить від інформації та інформаційних загроз, для кібербезпеки буде справедливо твердження: вона залежить від керованості системи. Адже чим більше керованості, чим точнішими будуть заходи щодо цієї керованості, а отже і захисту, і чим більше людина хоче затягти повідець, тим і значніші збитки від непередбачуваних обставин.

Неможливо передбачити всі обставини, навіть якщо працювати тисячу років над цим списком. Тому в кібербезпеці є декілька підходів, які б дозволили охопити максимально можливі зони майбутніх проблем. Одним з таких підходів є моделювання та прогнозування на основі отриманих раніше даних. Цей підхід використовується не тільки в контексті кібербезпеки, але й в інших сферах. Навіть при врахуванні майбутнього бюджету країни.

В цьому пункті метою є провести аналіз збитків, а також сфер та систем, де в майбутньому десятиліття виникнуть найбільші проблеми з боку НС на основі даних від Державної служби України з надзвичайних ситуацій. Це дозволить на основі реальної статистики прогнозувати сфери на можливі ситуації, які завдадуть шкоди обладнанню телемедицини та де і коли вона знадобиться перш за все. Адже основною задачею телемедицини є надання допомоги людям у будь-якій точці країни не зважаючи на умови середовища та віддаленість лікаря від пацієнтів.

3.3.1 Особливості збору даних для моделювання

В контексті моделювання надзвичайно важливими є вибір векторів, які будуть моделюватися. На основі цих векторів та даних, ми можемо зібрати інформацію за категоріями та більш ретельно її дослідити. Цей механізм носить назву вибірка даних.

Проте не слід вважати, що початкові задані вектори базуються лише на виборі авторів аналізу. Для якісного моделювання необхідно також враховувати, що задані напрямки, а також категорії, на які в подальшому буде розподілено інформацію, також беруться на основі тієї ж інформації. Це початковий аналіз.

Кожного календарного кварталу Державна служба України з надзвичайних ситуацій публікують на своєму офіційному сайті інформацію щодо офіційно зареєстрованих НС, а також жертв від них та збитків, які було задано.

В офіційній статистиці вже існують так звані категорії, що охоплюють всі НС. Якщо розглядати три глобальні категорії, то це: НС техногенного характеру, НС природнього характеру та НС соціального характеру. Кожна категорія розподілена на дрібніші підпункти, що дозволяє витрачати менше часу на пошук необхідних даних.

Ця офіційна статистика є джерелом більшості досліджень та саме на даних таких служб базується притаманна більшість дослідників.

Окрім категорій, що охоплюють НС, в даних служб також є короткий опис того, що саме це за НС та який вона мала наслідок. У числовій формі представлено кількість загиблих людей, у тис. грн. коштів, що потребувало усунення аварії, та регіони, де сталася трагедія.

Дані, представлені у звітах, стосуються як глобальних трагедій, таких як повені, аварії на заводах та тому подібне, так і суто локальних катастрофах як то дорожні пригоди чи різні правопорушення окремих цивільних. І якщо дані, що стосуються дрібних правопорушень, можуть бути затримані якимось з регіонів, тобто слід враховувати, що НС соціального характеру зазвичай занижені, то дані по глобальним ситуаціям передаються доволі чітко.

У Таблиці 3.3 представлені загальні дані за період з 2000 по 2010 роки, зібрані на основі категорії Державної служби України з надзвичайних ситуацій [13] та підбиті підсумки з економічних втрат.

Таблиця 3.3 - НС за характерами подій за 2000-2010 роки на території України та суми збитків від них

ВИД	Кількість	Сума збитків, тис.грн
1	2	3
НС ТЕХНОГЕННОГО ХАРАКТЕРУ		
НС унаслідок аварій чи катастроф на транспорті (за винятком пожеж і вибухів)	541	62703
НС унаслідок пожеж, вибухів	928	1015453
НС унаслідок аварій з викиданням (загрозою викидання) нхр, корисних копалин на інших об'єктах (окрім аварій на транспорті)	26	85
НС унаслідок наявності у навколишньому середовищі шкідливих (забруднювальних) і радіоактивних речовин понад гдк	124	76038
НС унаслідок аварій з викиданням (загрозою викидання) рр (крім аварій на транспорті)	3	0
НС унаслідок раптового руйнування будівель і споруд	120	101764
НС унаслідок аварій в електроенергетичних системах	277	41714
НС унаслідок аварій у системах життєзабезпечення	249	216210
НС унаслідок аварії систем телекомунікацій	21	2474
НС унаслідок аварій на очисних спорудах	8	20477
НС унаслідок аварій у системах нафтогазового промислового комплексу	2	125
НС техногенного характеру загалом	*2299*	*1537043*

Продовження таблиці 3.3

1	2	3
НС ПРИРОДНЬОГО ХАРАКТЕРУ		
Геофізичні НС	2	1028
Геологічні НС	117	467714
Метеорологічні НС	780	4681500
Гідрологічні морські НС	8	14478
Гідрологічні НС поверхневих вод	60	4845643
НС, пов'язані з пожежами в природних екологічних системах	157	106454
медико-біологічні НС	815	34366
НС природнього характеру загалом:	*1939*	*10151183*
НС СОЦІАЛЬНОГО ХАРАКТЕРУ		
Збройні напади, захоплення й утримування об'єктів державного значення (найбільш важливих та важливих державних об'єктів) або реальна загроза здійснення таких акцій	1	0
Посягання на життя державного чи громадського діяча	4	25
Встановлення вибухового пристрою у багатолюдному місці, установі (організації, підприємстві), житловому секторі, транспорті	42	36
НС, пов'язані з зникненням чи викраденням зброї та небезпечних речовин з об'єктів їх зберігання, використання, перероблення або під час транспортування	18	0
НС, пов'язані з нещасними випадками з людьми	156	802
НС соціального характеру загалом:	*221*	*863*
Загалом:	**4459**	**11689089**

3.3.2 Обробка даних за методом пріорітизації на базі матриці ризику

У загальному випадку оцінка ризику включає декілька етапів:

- ідентифікація ризиків як процес їх розпізнавання та опису;

- аналіз ризику, що передбачає осмислення природи ризику та визначення його рівня;

- оцінювання ризику, що передбачає порівняння результатів аналізу ризиків з критеріями для визначення, чи є ризик прийнятним або допустимим.

Якщо вирішується завдання запобігання та готовності до загрози певного типу, ризик може бути кількісно визначений як функція ймовірності виникнення загрози, експозиції (загальна вартість усіх елементів, що перебувають під впливом ризику) та уразливості (конкретний вплив на експозицію).

При цьому в країнах ЄС з метою проведення національної оцінки ризику (National Risk Assessment) для критичної інфраструктури рекомендується використовувати матрицю ризику розмірністю 5 х 5 як засіб для візуалізації результатів оцінки (Рис. 3.2).

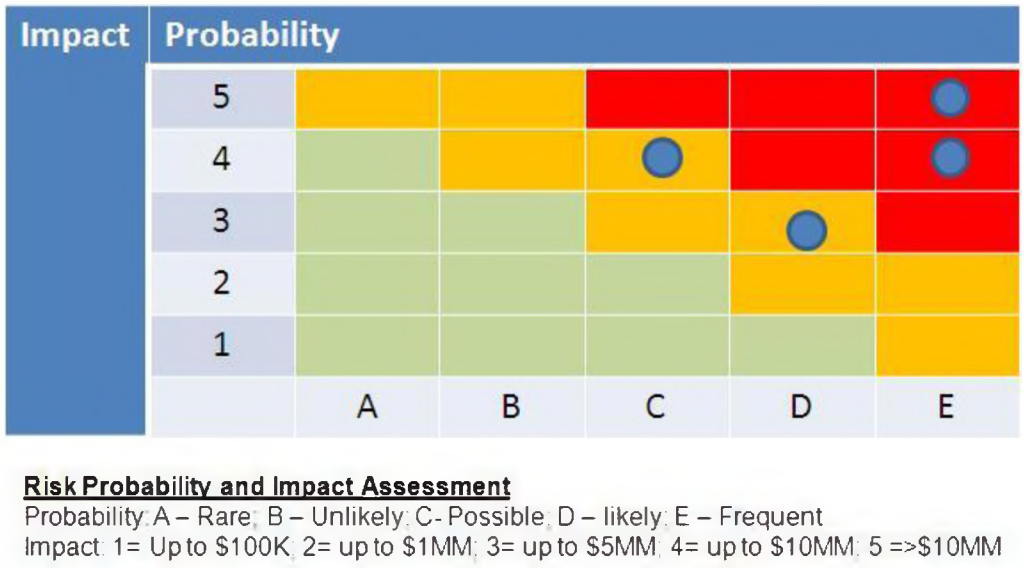

Рисунок 3.2 – Приклад матриці ризику

Оцінка ризиків повинна проводитися на основі трьох різних категорій впливу і враховувати негативні наслідки для людини (населення), економіки (та довкілля), а також політичні й соціальні наслідки. При цьому для перших двох категорій впливу негативні наслідки визначаються у кількісному вигляді як кількість загиблих (травмованих) осіб або економічних збитків у грн (євро). Наслідки для третьої категорії впливу, з огляду на соціальні та політичні взаємозв'язки, визначаються через якісні показники. [14]

У Європейському Союзі кожна країна має проводити оцінку ризиків для кожної категорії наслідків і відповідно будувати три різні матриці ризику при проведенні оцінки ризиків для критичної інфраструктури. Серед усіх загроз різного походження для безпеки критичної інфраструктури найбільш важливими визначено такі:

- природні: повені, екстремальні погодні явища, лісові пожежі, землетруси, епідемії та пандемії, епізоотії;

- техногенні: а) незловмисні: промислові аварії, ядерні/радіологічні аварії, аварії на транспорті, втрата критично важливої інфраструктури; б) зловмисні: кібератаки, терористичні атаки.

Усвідомлення каскадних ефектів сучасних загроз є досить складним через взаємозв'язок об'єктів інфраструктури та оточуючого її середовища. Неспроможність дійти згоди заінтересованих сторін і політичного керівництва у питаннях прогнозування та пом'якшення негативних наслідків новітніх загроз, насамперед природного походження, може призвести до серйозних порушень у роботі критичної інфраструктури в найближчому майбутньому.

Всі ці дані є також вірними і для наших ситуацій. На разі побудуємо матрицю ризику, базуючись на даних, що ми отримали раніше. У Таблиці 3 представлено оброблені дані з підписом точок, що будуть знаходитися на матриці ризику. В даному випадку вважаємо, що на осі X у нас стоїть числове значення, а саме ймовірність реалізації надзвичайної ситуації. Вона розраховується завдяки діленню кількості НС в одній категорії на загальну кількість НС.

На осі У позначено збитки, тобто вклад тієї чи іншої події в загальну суму збитків. Розраховується діленням значення збитку для однієї окремої ситуації на загальну суму збитків.

Таблиця 3.4 – Дані для побудови Рисунку 3.3

ВИД	Вісь Х	Вісь У	Точка
1	2	3	4
НС ТЕХНОГЕННОГО ХАРАКТЕРУ			
НС унаслідок аварій чи катастроф на транспорті (за винятком пожеж і вибухів)	0,12133	0,005364233	1
НС унаслідок пожеж, вибухів	0,20812	0,086871868	2
НС унаслідок аварій з викиданням (загрозою викидання) нхр, корисних копалин на інших об'єктах (окрім аварій на транспорті)	0,00583	7,27174E-06	3
НС унаслідок наявності у навколишньому середовищі шкідливих (забруднювальних) і радіоактивних речовин понад гдк	0,02781	0,006505041	4
НС унаслідок аварій з викиданням (загрозою викидання) рр (крім аварій на транспорті)	0,00067	0	5
НС унаслідок раптового руйнування будівель і споруд	0,02691	0,008705897	6
НС унаслідок аварій в електроенергетичних системах	0,06212	0,003568627	7
НС унаслідок аварій у системах життєзабезпечення	0,05584	0,018496737	8
НС унаслідок аварії систем телекомунікацій	0,00471	0,00021165	9
НС унаслідок аварій на очисних спорудах	0,00179	0,001751805	10
НС унаслідок аварій у системах нафтогазового промислового комплексу	0,00045	1,06937E-05	11
НС ПРИРОДНЬОГО ХАРАКТЕРУ			
Геофізичні НС	0,00045	8,79453E-05	12
Геологічні НС	0,02624	0,04001287	13
Метеорологічні НС	0,17493	0,400501699	14
Гідрологічні морські НС	0,00179	0,001238591	15
Гідрологічні НС поверхневих вод	0,01346	0,41454411	16
НС, пов'язані з пожежами в природних екологічних системах	0,03521	0,009107125	17

Продовження таблиці 3.4

1	2	3	4
Медико-біологічні НС	0,18278	0,002940007	18
НС СОЦІАЛЬНОГО ХАРАКТЕРУ			
Збройні напади, захоплення й утримування об'єктів державного значення (найбільш важливих та важливих державних об'єктів) або реальна загроза здійснення таких акцій	0,00022	0	19
Посягання на життя державного чи громадського діяча	0,0009	2,13875E-06	20
Встановлення вибухового пристрою у багатолюдному місці, установі (організації, підприємстві), житловому секторі, транспорті	0,00942	3,0798E-06	21
НС, пов'язані з зникненням чи викраденням зброї та небезпечних речовин з об'єктів їх зберігання, використання, перероблення або під час транспортування	0,00404	0	22
НС, пов'язані з нещасними випадками з людьми	0,03499	6,8611E-05	23

Далі буде побудовано Залежність між ймовірностями виникнення НС та загибелі від НС. Цей графік при накладанні на матрицю ризику показує нам рівні загроз та, по суті, без складних аналітичних робіт дозволяє провести глибокий аналіз по пріорітизації загроз.

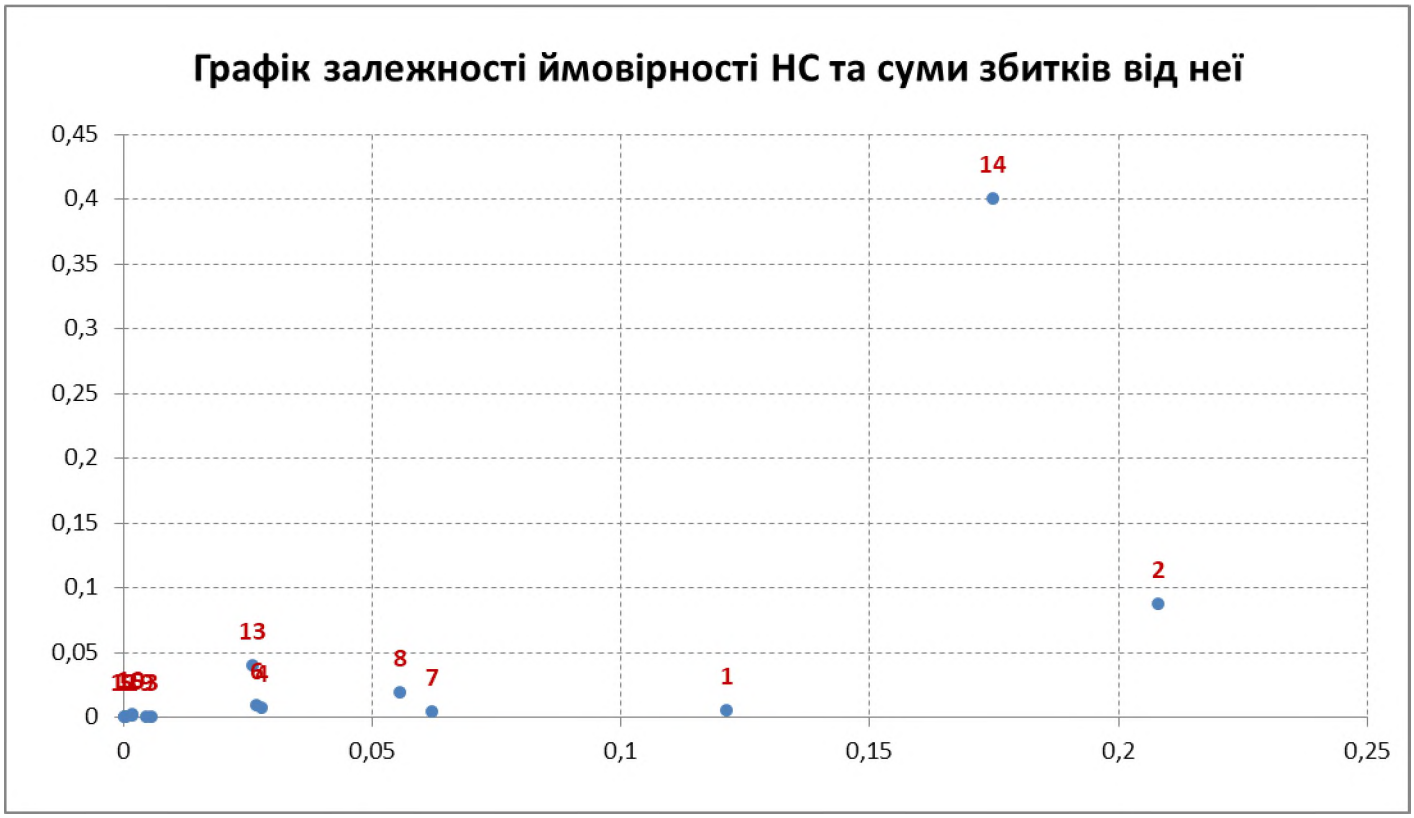

Рисунок 3.3 – Графік залежності

Для подальшого аналізу нам навіть не потрібно будувати матрицю, оскільки на графіку доволі чітко видно дві точки, що мають найбільший вплив.

Це точка №14 – Метеорологічні НС, та точка №2 – НС у наслідок пожеж і вибухів.

На базі цих даних ми можемо чітко виділити загрози, які будуть актуальними і не тільки забезпечити захист телемедичного обладнання, проте і виділити точки, де знадобляться телемедичні послуги.

Також слід зазначити, що дана статистика існує не тільки в узагальненому виді для всієї території України, проте і для кожного окремого регіону, що дозволить покращити прогнозування. Також можна взяти свіжіші дані, зробивши вибірку ще більшою.

Виходячи з оцінки, на Рисунку 3.3 ми бачимо види загроз, які можуть трапитися, та збитки від них. Виходячи з даних умов, ризик було оцінено для бальної шкали за матричним методом.

3.4 Інформаційна складова ризиків

У цьому пункті мова буде йти безпосередньо про оцінку системи телемедицни та різноманітні математичні моделі, а також способи, як саме за краще дослідити цю систему.

Як було описано у Розділах 1 та 2, для побудови математичних моделей доволі складно використовувати однозначні числа, які були б закріплені у звичайній математиці. Тому тут використовується нечіткий вивід, нечітка множина, нечіткі числа та нечітка логіка.

Для того, щоб дослідити ризик для системи, перш за все необхідно дослідити саму систему і провести оцінку стану захищеності. Система телемедицини є складною системою, що сама по собі включає багато пунктів та підпунктів. Як не існує єдиної системи класифікацій, так не існує й уніфікованої системи оцінки чи методики, як її проводити.

Далі приведено один з методів аналізу ризику катастрофічної події, який буде видавати в результаті лінгвістичну змінну як висновок щодо оцінки складної системи та всіх її можливостей. Цей алгоритм є економічним методом, що використовується при проведені аналізи ризику банкротства фірми в кожному з поточних кварталів. Його можна використовувати для побудови моди та економічного аналізу тенденцій розвитку системи.

В роботі приведено результат аналізу стану на сьогоднішній час, а саме кінець 2018 року, виходячи з опису телепроцедур, типових загроз для них та інших даних, зібраних у Розділах 1-2 роботи.

3.4.1 Обґрунтування доцільності використання методу

Проведення оцінки стану захищеності системи дасть лінгвістичну змінну, яка описує систему. У ній вказано засоби захисту системи і вірогідності того, що буде проведено успішну реалізацію проникнення в систему.

Однією з варіантів формул для обрахунку ризику є пряма формула. Для обрахунку прямого ризику використовується:

$$R = P_1 * P_2 * P_3$$

Де у нас P_1 – ймовірність формування небезпечного явища процесу, що може представляти загрозу для об'єкту ризику.

P_2 – вірогідність того, що рівень ризик-утворюючого фактору буде достатній для створення катастрофічного впливу на об'єкт ризику.

P_3 – ймовірність того, що фактор дійсно призведе до катастрофічних явищ для об'єкту ризику.

У даній формулі добуток $(P_2 * P_3)$ – включає в себе збиток від катастрофи та може бути пере позначений як $Q_{\text{катастр.}}$

Виходячи з пояснень до даного підходу оцінки ризику, побачимо, що вона практично повністю ґрунтується на самій системі, а не на можливих зовнішніх загрозах. Для успішного обрахунку необхідно використати дані системи та експертні оцінки системи.

Цей метод як ніщо краще лягає в основу алгоритму, використаного далі, що також цілком і повністю є продуктом аналізу самої системи та експертних оцінок до неї.

3.4.2 Задача аналізу ризику при проведені телемедичних процедур

Для прикладу використання алгоритму детально проведено оцінку однієї з телепроцедур, а саме телехірургії. Результати аналізу кожної з телепроцедур знаходяться в таблиці в кінці розділу.

Дана задача є модифікацією задачі аналізу ризику банкрутства с курсу економіки [12].

Крок 1. Для кількісної оцінки стану захищеності об'єкта захисту на 1 кроці розглядають лінгвістичні змінні. Це дозволить уникнути неприємностей зі спробами чіткого визначення чисел і помилками чи протиріччями при вирішенні питань у різних експертів. Тут слід вважати, що саме завдяки цьому пункту можна в подальшому адаптувати цю модель під будь-які інші умови.

Задамо лінгвістичну змінну g = «ризик припинення функціонування телемедичної процедури». Ця змінна розуміє під собою будь-яку причину, через яку може статися зрив процедури. Тут вважається і компрометування інформації, і пошкодження обладнання, і дії зловмисника, що можуть призвести до загрози для кінцевого споживача.

Після завдання змінної розглядається універсальна множина [0,1]

$G = \{G_1, G_2, G_3, G_4, G_5\}$, де

G_1= «граничний ризик припинення функціонування телемедичної процедури»

G_2= «степінь ризику припинення функціонування телемедичної процедури висока»

G_3= «степінь ризику припинення функціонування телемедичної процедури середня»

G_4= «степінь ризику припинення функціонування телемедичної процедури низька»

G_5= «ризику припинення функціонування телемедичної процедури незначний»

Ця множина в результаті охоплює повну групу подій, яка можлива в разі виникнення загрози чи виявлення уразливості. Звичайно, це доволі спрощений варіант, проте для більш детального розгляду можна гнучко додати декілька змінних у цю множину і збільшити кількість лінгвістичних змінних.

Крок 2. Складаємо графік функції приналежності для кожного терма (Рис. 3.4) використовуючи аналітичний вираз для функціональної приналежності трапецеїдального нечіткого числа.

$$X = A_1, A_2, A_3, A_4, A_5$$

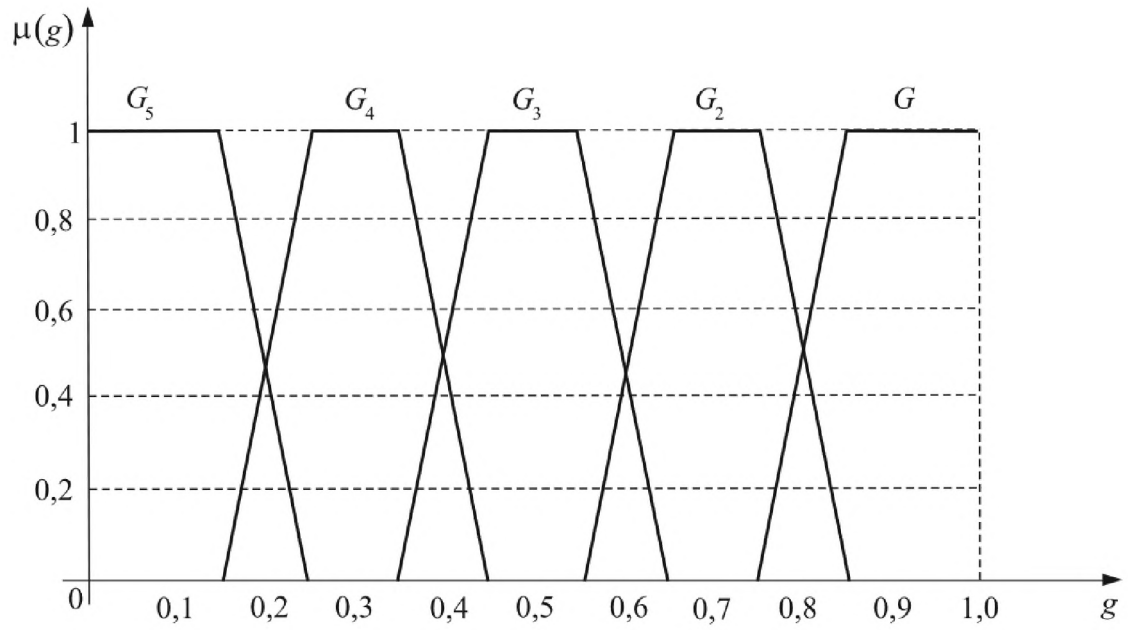

Рисунок 3.4 – Функції розподілу термів на універсальній множині

$$\mu(x) = \begin{cases} 0, & \text{якщо } x < a_1, \quad x > a_4 \\ \dfrac{x - a_1}{a_2 - a_1}, & \text{якщо } a_1 \le x < a_2 \\ 1, & \text{якщо } a_2 \le x < a_3 \\ \dfrac{x - a_4}{a_3 - a_4}, & \text{якщо } a_3 \le x < a_4 \end{cases}$$

Крок 3. Будуємо таблицю 3.5, виходячи з даних, наведених на Кроці 2

Таблиця 3.5 – Відповідність термів та функцій приналежності

Терми G_i	Функція приналежності μ_i
G_5= «ризику припинення функціонування телемедичної процедури незначний»	$\mu_5 = \begin{cases} 1, \text{якщо } 0 \le g \le 0{,}15 \\ 10(0{,}25 - g), \text{якщо } 0{,}15 \le g \le 0{,}25 \end{cases}$
G_4= «степінь ризику припинення функціонування телемедичної процедури низька»	$\mu_4 = \begin{cases} 1 - 10(0{,}25 - g), \text{якщо } 0{,}15 \le g \le 0{,}25 \\ 1, \text{якщо } 0{,}25 \le g \le 0{,}35 \\ 10(0{,}45 - g), \text{якщо } 0{,}35 \le g \le 0{,}45 \end{cases}$
G_3= «степінь ризику припинення функціонування телемедичної процедури середня»	$\mu_3 = \begin{cases} 1 - 10(0{,}45 - g), \text{якщо } 0{,}35 \le g \le 0{,}45 \\ 1, \text{якщо } 0{,}45 \le g \le 0{,}55 \\ 10(0{,}65 - g), \text{якщо } 0{,}55 \le g \le 0{,}65 \end{cases}$
G_2= «степінь ризику припинення функціонування телемедичної процедури висока»	$\mu_2 = \begin{cases} 1 - 10(0{,}65 - g), \text{якщо } 0{,}55 \le g \le 0{,}65 \\ 1, \text{якщо } 0{,}65 \le g \le 0{,}75 \\ 10(0{,}85 - g), \text{якщо } 0{,}75 \le g \le 0{,}85 \end{cases}$
G_1= «граничний ризик припинення функціонування телемедичної процедури»	$\mu_1 = \begin{cases} 1 - 10(0{,}85 - g), \text{якщо } 0{,}75 \le g \le 0{,}85 \\ 1, \text{якщо } 0{,}85 \le g \le 1 \end{cases}$

Крок 4. Значення функцій приналежності ми розглянемо як істинність термів G_i.

Наприклад, якщо g = 0,62 було встановлено, то відмінну від 0 функцію належності мають 2 терми: G_3= «степінь ризику припинення функціонування телемедичної процедури середня» і G_2= «степінь ризику припинення функціонування телемедичної процедури висока».

Тоді $$\mu_3(0{,}62) = 10(0{,}65 - g)|_{0{,}62} = 0{,}3$$

$$\mu_2(0{,}62) = 1 - 10(0{,}65 - g)|_{0{,}62} = 0{,}7$$

Таким чином для g = 0,62 вислів степінь ризику припинення функціонування телемедичної процедури висока» є більш істинним, оскільки 0,7 більше ніж 0,3 і вислів «степінь ризику припинення функціонування телемедичної процедури середня».

Крок 5. Висновок про ризик припинення функціонування телемедичної процедури експерт робить на основі аналізу показників підприємства. Ці показники вибираються наступним чином:

зростання кожного окремого показника X_i повинно бути пов'язано зі зменшенням ступеня ризику припинення функціонування телемедичної процедури. Тобто ці показники повинні бути спрямовані на поліпшення мір безпеки в телемедичних процедурах.

Експерт вибрав наступні показники для телехірургії:

X_1 = «коефіцієнт автономії». Це визначає здатність системи функціонувати незалежно від зовнішніх джерел (енергія, мережа, інші ресурси).

X_2 = «коефіцієнт внутрішніх засобів захисту». Цей пункт включає системи внутрішнього захисту, такі як паролі персональних комп'ютерів, системи антивірусів та інше.

X_3 = «коефіцієнт зовнішньої захищеності системи». Визначає такі фактори як брандмауер, захист каналів передачі даних, КЗ та інше.

X_4 = «коефіцієнт надійності програмного забезпечення». Цей пункт стосується програмних оболонок систем та всіх їх компонентів.

X_5 = «коефіцієнт надійності апаратури». Стосується усього обладнання, що використовується у ході процедур телемедицини.

X_6 = «коефіцієнт надійності співробітників». Цей пункт стосується персоналу, що працює і обслуговує систему. В тому числі їх здатність протидії соціальній інженерії.

Крок 6. Кожний фіксований показник є чіткою ймовірнісною змінною, що приймає свої значення на деякому чисельному проміжку, тому кожну з цих числових змінних будемо розглядати як множину лінгвістичних змінних B_i які складаються із наступних термів:

B_{i1} = «дуже низький рівень показника X_i»

B_{i2} = «низький рівень показника X_i»

B_{i3} = «середній рівень показника X_i»

B_{i4} = «високий рівень показника X_i»

B_{i5} = «дуже високий рівень показника X_i»

Крок 7. Таким чином, ми прийняли, що кожна дана лінгвістична змінна має трапецеїдальну функцію приналежності, що характеризується 4 числами a_1, a_2, a_3, a_4, які встановлюються експертами. Ці дані ми заносимо до таблиці 3.6.

Таблиця 3.6 – Залежність показників приналежності від термів

Показники	Терми				
	B_{i1}	B_{i2}	B_{i3}	B_{i4}	B_{i5}
X_1	a_1, a_2 a_3, a_4	a_1, a_2 a_3, a_4	a_1, a_2 a_3, a_4	a_1, a_2 a_3, a_4	a_1, a_2 a_3, a_4
. . .	. . .	. . .	. . .	. . .	. . .

Ці чотири числа є не що інше, як експертні оцінки, що стосуються показників X_i. Таким чином, експерти заповнюють таблицю і на основі цим трапецеїдальних чисел проводять подальший аналіз.

Тут також можна використати різні методи для покращення результатів узгодженості за рахунок декількох послідовних ітерацій за

У Таблиці 3.7 представлено експертні оцінки для телехірургії.

Таблиця 3.7 – Експертні оцінки якісних показників для телехірургії

Показники	Терми				
	B_{i1}	B_{i2}	B_{i3}	B_{i4}	B_{i5}
X_1	(0; 0; 0.1; 0.2)	(0.1; 0.2; 0.25; 0.3)	(0.25; 0.3; 0.35; 0.4)	(0.3; 0.4; 0.55; 0.7)	(0.55; 0.7; ∞; ∞)
X_2	(0; 0; 0.1; 0.11)	(0.1; 0.11; 0.3; 0.35)	(0.3; 0.35; 0.4; 0.45)	(0.4; 0.45; 0.5; 0.51)	(0.5; 0.51; 1; 1)
X_3	(0; 0; 0.1; 0.2)	(0.1; 0.2; 0.3; 0.4)	(0.3; 0.4; 0.5; 0.6)	(0.5; 0.6; 0.7; 0.8)	(0.7; 0.8; 1; 1)
X_4	(0; 0; 0.2; 0.4)	(0.2; 0.4; 0.5; 0.6)	(0.5; 0.6; 0.7; 0.8)	(0.7; 0.8; 0.85; 0.9)	(0.8; 0.9; 1; 1)
X_5	(0; 0; 0.25; 0.35)	(0.25; 0.35; 0.5; 0.6)	(0.5; 0.6; 0.7; 0.75)	(0.7; 0.75; 0.8; 0.85)	(0.8; 0.85; 1; 1)
X_6	(-1; -1; 0; 0)	(0; 0; 0.15; 0.3)	(0.1; 0.3; 0.4; 0.45)	(0.4; 0.45; 0.5; 0.6)	(0.5; 0.6; 1; 1)

Для Таблиці 3.7 діють ті ж самі правила, які було описано в прикладі на Кроці 4. Тобто, наприклад:

Якщо у нас X_5 = 0.72, то стан цього показника може бути визначений як:

B_{53} = (0.4; 0.6; 0.7; 0.75) - «середній рівень показника X_5» або як B_{54} = (0.7; 0.75; 0.8; 0.85) - «високий рівень показника X_5». При цьому $\mu_{53} = \frac{x-0.75}{0.7-0.75}|_{x=0.72} = \frac{-0.03}{-0.05} = 0.6$ – оцінка істинності для B_{53}; $\mu_{54} = \frac{x-0.7}{0.75-0.7}|_{x=0.72} = \frac{0.02}{0.05} = 0.4$ – оцінка істинності для B_{54}. Тобто вираз B_{53} є більш істинним для X_5 = 0.72.

Крок 8. Тепер у нас необхідно перейти від фінансових показників X_i до змінних G_1. Для цього необхідно проранжувати показники по ступені їх внеску в ризик припинення функціонування телемедичної процедури. Тобто кожному X_i поставити у відповідність $X_i \to r_i$ ранг, який визначатиме міру припинення функціонування телемедичної процедури.

Для цього, якщо ми визначимо $r_1 \geq r_2 \geq \cdots \geq r_n$

Можна скористатися шкалою Фішберна, яка:

$r_i = \frac{2(n-i+1)}{n(n-1)}$ - формула Фішберна.

Формула Фішберна відповідає максимальній ентропії наявної інформації невизначеності про об'єкт дослідження. Якщо ми вважаємо, що показники рівно визначенні або в системі переваг немає, то вони мають наступний вигляд: $r_i = \frac{1}{n}$.

Крок 9. Для вибраної нами системи показників правило переходу від значень X_i показників до ваг термів лінгвістичної змінної g має наступний вигляд:

$$p_k = \sum_{i=1}^{G} r_i * \mu_{ki}, \quad k = \overline{1,5}$$

Розрахувавши необхідні ваги для кожного терму змінної G_i отримаємо значення:

$$g = \sum_{k=1}^{G} p_k * \overline{g_k}$$

При цьому $\overline{g_k}$ – є середина проміжку, який є носієм терма $G_k = (a_{k1},\ a_{k4}]$ як показано на Рисунку 3.5.

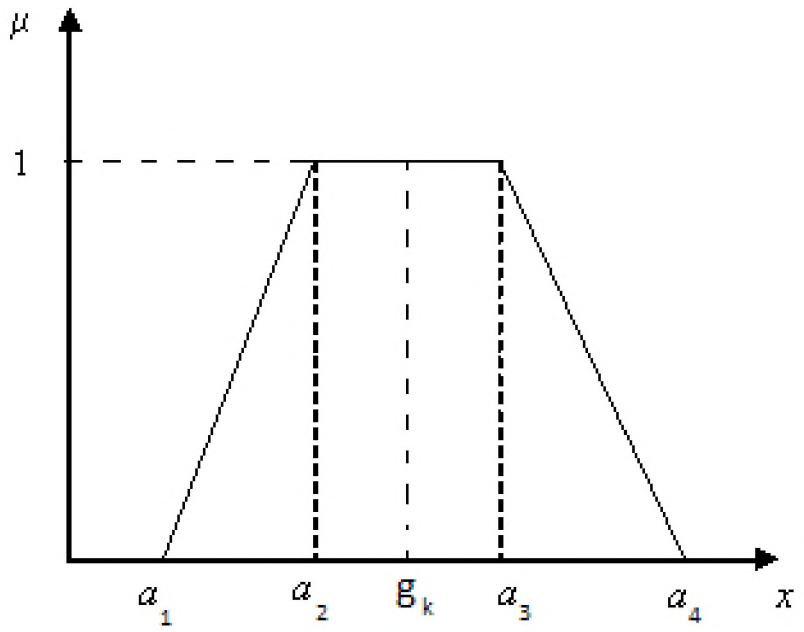

Рисунок 3.5 – Середина інтервалу $\overline{g_k}$

На Рисунку 3.5 ми бачимо трапецеїдальне число, а саме ті 4 значення а, які були нам наведені у Таблиці 3.6. Середина цього інтервалу є серединою до інтервалів функції приналежності μ_i.

Будуємо правило переходу на Рисунку 3.6.

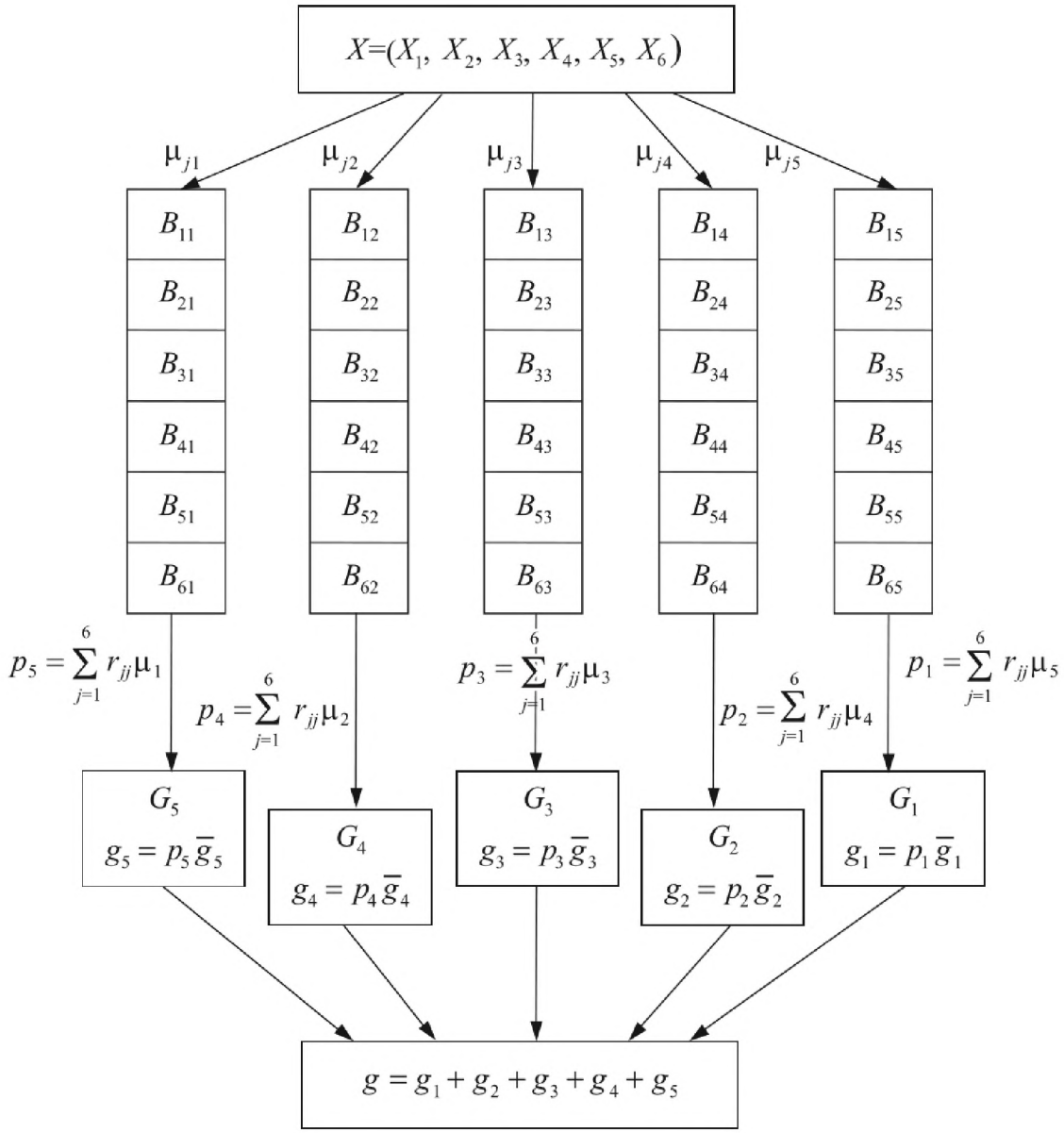

Рисунок 3.6 – Схема переходу від показників X_i до висловів щодо степінь ризику припинення функціонування телемедичної процедури

Крок 10. Тепер ми маємо таблицю експертних оцінок і можемо безпосередньо оцінити систему за показниками X_i, які ми маємо із дослідження телемедичних процедур у Розділі 2.

У Таблиці 3.8 наведено первинну обробку даних для задачі.

Таблиця 3.8 – Первинні дані показників X_i для телехірургії

Спостережувані значення показників на кінець 2018 року	Рівень показника (трапецеїдальне число)	Значення функції приналежності
X_1 = 0.15	B_{11} = (0; 0; 0.1; 0.2) B_{12} = (0.1; 0.2; 0.25; 0.3)	$\mu_{11} = 0.5$ $\mu_{12} = 0.5$
X_2 = 0.6	B_{25} = (0.5; 0.51; 1; 1)	$\mu_{25} = 1$
X_3 = 0.52	B_{33} = (0.3; 0.4; 0.5; 0.6) B_{34} = (0.5; 0.6; 0.7; 0.8)	$\mu_{33} = 0.8$ $\mu_{34} = 0.2$
X_4 = 0.42	B_{42} = (0.2; 0.4; 0.5; 0.6)	$\mu_{42} = 1$
X_5 = 0.62	B_{53} = (0.5; 0.6; 0.7; 0.75)	$\mu_{53} = 1$
X_6 = 0.42	B_{63} = (0.1; 0.3; 0.4; 0.45) B_{64} = (0.4; 0.45; 0.5; 0.6)	$\mu_{63} = 0.6$ $\mu_{64} = 0.4$

Тепер ми можемо обрахувати лінгвістичну змінну і зробити остаточний вивід щодо ризику припинення функціонування телепроцедури телехірургії, використовуючи схему, зображену на Рисунку 3.6. Усі необхідні дані заносимо до Таблиці 3.9.

Таблиця 3.9 – Обчислення значення функції приналежності лінгвістичної змінної g = «ризик припинення функціонування телемедичної процедури».

Вага терма p_i лінгвістичної змінної g	Множина носіїв і -ого терма лінгвістичної змінної g	Середина проміжку $G_i, \overline{g_i}$	$g_i = p_i \overline{g_i}$
$p_5 = \sum_{j=1}^{6} r_j \mu_{j1} = \frac{1}{6}\mu_{11} = \frac{1}{6} * 0.5 \approx 0.083$	$G_5 \in [0; 0.25]$	0.125	0.0104
$p_4 = \sum_{j=1}^{6} r_j \mu_{j2} = \frac{1}{6}(\mu_{12} + \mu_{42}) = \frac{1}{6}(0.5 + 1) = 0.25$	$G_4 \in (0.15; 0.45]$	0.3	0.075
$p_3 = \sum_{j=1}^{6} r_j \mu_{j3} = \frac{1}{6}(\mu_{33} + \mu_{53} + \mu_{63}) = \frac{1}{6}(0.8 + 1 + 0.6) = 0.4$	$G_3 \in (0.35; 0.65]$	0.5	0.2
$p_2 = \sum_{j=1}^{6} r_j \mu_{j4} = \frac{1}{6}(\mu_{34} + \mu_{64}) = \frac{1}{6}(0.2 + 0.4) = 0.1$	$G_2 \in (0.55; 0.85]$	0.7	0.07
$p_1 = \sum_{j=1}^{6} r_j \mu_{j5} = \frac{1}{6}\mu_{25} = \frac{1}{6} * 1 \approx 0.167$	$G_1 \in [0.75; 1]$	0.875	0.146
$g = \sum_{i=1}^{5} g_i = 0.5014$			

Використовуючи Таблицю 3.9 знайдемо приналежність $\mu_k(g)$ для g=0.5014:

$$\mu_3(0.5014) = 1|_{g=0.5014}$$

і $\mu_k = 0$ при k=1, 2, 4, 5.

Опис стану телехірургії на кінець 2018-ого року: $G_3\,(\mu_3 = 1)$: «степінь ризику припинення функціонування телемедичної процедури середня».

В ході роботи у Розділах 1-2 було визначено 6 телемедичних процедур, для яких буде проведено оцінку за критерієм: g = «ризик припинення функціонування телемедичної процедури». Результати обрахунку кожного з показників представлено у Таблиці 3.9.

Послідовно виконуємо усі крови знову для кожної телепроцедури.

В результаті експерти будуть давати нам 20 різних четвірок чисел як у Таблиці 3.7, після чого ми будемо проводити оцінки кожної з систем, базуючись на їх показниках X_i.

Оскільки у нас усі процедури належать до телемедицини і є однією системою, ми можемо не міняти ці лінгвістичні змінні для кожної з телепроцедур.

Далі ми знову проводимо роботу з вагами, як показано на Рисунку 3.6.

Початкові значення нашої універсальної множини залишаються без змін.

Дана задача комфортна тим, що її можна використати не лише для обрахунку стану системи у поточний час, проте і з новими даними, якщо такі будуть виникати у подальшому.

Використовуючи дані за певний період, ми можемо побудувати моду та розглянути тенденцію розвитку ризиків у телемедицині.

У Таблиці 3.10 представлено 6 телемедичних процедур та значення трапецеїдального числа для них, а також результуючий висновок по кожній з процедур.

Таблиця 3.10 – Результати оцінки ризиків для телемедичних процедур станом на кінець 2018-ого року на території України

Телемедичні процедури	*Значення* $\mu_k(g)$	*Висновок*
1	2	3
Телемедичне консультування	$\mu_3(0.642) = 10(0.65 - 0.642)\|_{g=0.642}$ =0.05 $\mu_2(0.642) = 1 - 10(0.65 - 0.642)\|_{g=0.642}$ =0.95	G_3 ($\mu_3 = 0.05$): «степінь ризику припинення функціонування телемедичної процедури середня» $G_2(\mu_2 = 0.95)$: «степінь ризику припинення функціонування телемедичної процедури висока»
Біотелеметрія (телемоніторинг)	$\mu_4(0.312) = 1\|_{g=0.312}$	$G_4(\mu_4 = 1)$: «степінь ризику припинення функціонування телемедичної процедури низька»
Домашня (індивідуальна) телемедицина	$\mu_4(0.423) = 10(0.45 - 0.423)\|_{g=0.423}$ =0.27 $\mu_3(0.423) = 1 - 10(0.45 - 0.423)\|_{g=0.423} =$ = 0.73	$G_4(\mu_4 = 0.27)$: «степінь ризику припинення функціонування телемедичної процедури низька» G_3 ($\mu_3 = 0.73$): «степінь ризику припинення функціонування телемедичної процедури середня»

Продовження таблиці 3.10

1	2	3
Телескринінг	$\mu_4(0.4306) = 10(0.45 - 0.4306)\|_{g=0.4306}$ =0.194 $\mu_3(0.4306) = 1 - 10(0.45 - 0.4306)\|_{g=0.4306}$ =0.806	$G_4(\mu_4 = 0.194)$: «степінь ризику припинення функціонування телемедичної процедури низька» $G_3\,(\mu_3 = 0.806)$: «степінь ризику припинення функціонування телемедичної процедури середня»
Телеприсутність /телеасистування /телехірургрія	$\mu_3(0.5014) = 1\|_{g=0.5014}$	$G_3\,(\mu_3 = 1)$: «степінь ризику припинення функціонування телемедичної процедури середня»
Дистанційне навчання	$\mu_3(0.622) = 10(0.65 - 0.622)\|_{g=0.622}$ =0.28 $\mu_2(0.622) = 1 - 10(0.65 - 0.622)\|_{g=0.622}$ =0.72	$G_3\,(\mu_3 = 0.28)$: «степінь ризику припинення функціонування телемедичної процедури середня» $G_2(\mu_2 = 0.72)$: «степінь ризику припинення функціонування телемедичної процедури висока»

Висновки до розділу 3

У даному розділі ми провели оцінку ризиків за трьома різними факторами та методами. Кожен з них може вважатися складовою математичної моделі для проведення дослідження та, об'єднавшись, комплексу досліджень для покращення стану захищеності та зниженню ризику при проведенні телепроцедур.

На основі проведеної описової роботи в Розділах 1 та 2 було побудовано описово-математичну оцінку ризиків ІБ для телемедичних процедур, яка базується на трьох складових частинах ризику для телемедицини.

Для кінцевого споживача наведено дані у табличному варіанті для кращого розуміння ризику, на який він може спиратися, визначаючись, хочу проводити лікування за допомогою даної системи чи ні. Представлено дані в Таблиці 3.10, що базуються на технологіях проведення кожної з телепроцедур. Використано середні значення захищеності.

4 ПРАКТИЧНЕ ЗАСТОСУВАННЯ ОТРИМАНИХ ДАННИХ (СТАРТАП)

Стартап є практичною частиною роботи, яка доводить, що теоретичні викладки в Розділах 1-3 є корисними на практиці та можуть бути застосовані не лише у наукових цілях.

Цей розділ описує в собі ідею продукту, заснованого на дипломному завданні. Продукт: комплекс програм для оцінки ризиків ІБ телепроцедур.

Цей продукт є не що інше як комп'ютерна система, що дозволить проводити автоматизоване тестування, базуючись на заданому шаблоні, для телемедичних процедур та компаній, що на них спеціалізуються.

У продукту є дві основні гілки.

Перша – для кінцевого споживача чи звичайних людей. Ця гілка заснована на бажанні людини бути впевненою у тому, яку послугу вона отримує і чи є телемедицина безпечною.

Друга гілка – для компаній. За допомогою цього напряму компанії зможуть провести власний аудит, не використовуючи великих коштів.

4.1 Опис ідеї стартап-проекту

В межах підпункту слід послідовно проаналізувати та подати у вигля-ді таблиць:

- зміст ідеї (що пропонується);
- можливі напрямки застосування;
- основні вигоди, що може отримати користувач товару (за кожним напрямком застосування);
- чим відрізняється від існуючих аналогів та замінників.

Дані щодо опису ідеї стартап-проекту подано у Таблиці 4.1. У ній також наведено інформацію щодо напрямку застосування та вигоди для споживача.

Таблиця 4.1 – Опис ідеї стартап-проекту

Зміст ідеї	*Напрямки застосування*	*Вигоди для користувача*
Програмна платформа, що проводить швидкий автоматизований аналіз за попередньо заданими показниками.	1. Прямий напрямок для споживача	Користувач може оцінити ризик при використанні тієї чи іншої телепроцедури
	2. Прямий напрямок для фірми	Компанія може оцінити запропоновані нею послуги та спробувати знизити ризики для користувача
	3. Оцінка стану захищеності	На основі оцінки ризиків компанія може покращити власні технології та закрити слабкі місця системи, щоб уникнути більших збитків у майбутньому
	4. Рекламний для фірми	Виставивши свої оцінки, компанія може приваблювати нових клієнтів та конкурувати з іншими фірмами на ринку
	5. Популяризація для споживача	Оскільки телемедицина є спеціалізованою гілкою медицини, вона допомагає рятувати життя і її популяризація, а також звернення уваги на неї, є вкрай вигідними для здоров'я усіх людей

Аналіз потенційних техніко-економічних переваг ідеї (чим відрізняється від існуючих аналогів та замінників) порівняно із пропозиціями конкурентів передбачає:

- визначення переліку техніко-економічних властивостей та характеристик ідеї;

- визначення попереднього кола конкурентів (проектів-конкурентів) або товарів-замінників чи товарів-аналогів, що вже існують на ринку, та проводиться збір інформації щодо значень техніко-економічних показників для ідеї власного проекту та проектів-конкурентів відповідно до визначеного вище переліку;
- проводиться порівняльний аналіз показників: для власної ідеї визначаються показники, що мають а) гірші значення (W, слабкі); б) аналогічні (N, нейтральні) значення; в) кращі значення (S, сильні).

У Таблиці 4.2 представлено усі показники щодо стану проекту.

Продукт не має аналогів на ринку. В якості найближчих конкурентів можуть виступати агентства, що проводять аудит інформаційної безпеки (DATAMI) = Конкурент 1 в Таблиці 4.2, система оцінки уразливостей (CVSS) = Конкурент 2 в Таблиці 4.2.

Таблиця 4.2 - Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	*Техніко-економічні характеристики ідеї*	*(Потенційні) товари/концепції конкурентів*			*W (слабка сторона)*	*N (нейтральна сторона)*	*S (сильна сторона)*
		Мій проект	*Конкурент1*	*Конкурент2*			
1.	Економічна	Дешева система ПЗ	Складний комплекс та система	Дешева платформа		+	
2.	Надійність	Надійний результат	Надійний результат	Середній результат			+
3.	Технологічність	висока	висока	низька			+
4.	Безпека	висока	висока	низька		+	
5.	Призначення	висока	низька	низька		+	

4.2 Технологічний аудит ідеї проекту

В межах даного підрозділу необхідно провести аудит технології, за допомогою якої можна реалізувати ідею проекту (технології створення товару).

Визначення технологічної здійсненності ідеї проекту передбачає аналіз таких складових:

- за якою технологією буде виготовлено товар згідно ідеї проекту?
- чи існують такі технології, чи їх потрібно розробити/доробити?
- чи доступні такі технології авторам проекту?

За результатами аналізу таблиці робиться висновок щодо можливості технологічної реалізації проекту: так чи ні, а також технологічного шляху, яким це доцільно зробити (з поміж названих технологій обираються такі, що доступні авторам проекту та є наявними на ринку).

У Таблиці 4.3 представлено дані для проведення аудиту.

Таблиця 4.3 – Технологічна здійсненність ідеї проекту

№ п/п	*Ідея проекту*	*Технології її реалізації*	*Наявність технологій*	*Доступність технологі1*
1	Написання платформи для продукту	Написання на мові програмування	Технологія наявна	У вільному доступі
2	Написання шаблону	Систематизація на псевдокоді	Технологія наявна	У вільному доступі
3	Збір даних для розширення системи	Автоматизований збір даних з оцінок користувачів	Технологія наявна	Технологія доступна після надання дозволу фірмами
Обрана технологія реалізації ідеї проекту: всі три технології є доступними та мають свої сильні та слабку сторони. Обрано 1-шу технологію: написання на мові програмування.				

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть пере-шкодити реалізації проекту, дозволяє спланувати напрями розвитку про-екту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів.

У Таблиці 4.4 представлено дані щодо аналізу попиту: наявність попиту, обсяг, динаміка розвитку ринку. Середня норма рентабельності в галузі (або по ринку) порівнюється із банківським відсотком на вкладення. За умови, що останній є вищим, можливо, має сенс вкласти кошти в інший проект.

За результатами аналізу таблиці робиться висновок щодо того, чи є ринок привабливим для входження за попереднім оцінюванням.

Таблиця 4.4 - Попередня характеристика потенційного ринку стартап-проекту

№ п/п	*Показники стану ринку (найменування)*	*Характеристика*
1	Кількість головних гравців, од	10
2	Загальний обсяг продаж, грн/ум.од	10000
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Репутаційне обмеження можливе
5	Специфічні вимоги до стандартизації та сертифікації	Законодавча база України
6	Середня норма рентабельності в галузі (або по ринку), %	80%

Надалі визначаються потенційні групи клієнтів, їх характеристики, та формується орієнтовний перелік вимог до товару для кожної групи, що представлено у Таблиці 4.5.

Таблиця 4.5 - Характеристика потенційних клієнтів стартап-проекту

№ п/п	*Потреба, що формує ринок*	*Цільова аудиторія (цільові сегменти ринку)*	*Відмінності у поведінці різних потенційних цільових груп клієнтів*	*Вимоги споживачів до товару*
1	Соціальна потреба	Кінцевий споживач	Поведінку клієнта формує страх та недовіра до телемедицини. Стандарти України, а також закон України про телемедицину.	До продукції: швидка дія та простота у використанні. До компанії: гарантія та прозорість усіх обрахунків, точність результатів у межі заданої похибки
2	Технічна потреба	Клініки, госпіталі, приватні лікарні	Поведінку клієнта формує популярність телемедини та спроби популяризації власних компаній	До продукції: популярність використання, широка можливість шаблонів. До компанії: анонімність проведення тестування та гарантії точності оцінок у рамках похибки

Після визначення потенційних груп клієнтів проводиться аналіз ринкового середовища: складаються таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому перешкоджають. Це представлено у Таблицях 4.6 і 4.7. Фактори в таблиці подавати в порядку зменшення значущості.

Таблиця 4.6. - Фактори загроз

№ п/п	*Фактор*	*Зміст загрози*	*Можлива реакція компанії*
1	Недовіра клієнта	Оскільки така ідея є сміливою, клієнти можуть не довіряти результатам	Проводження консультацій з клієнтами, відповіді на питання, математичні обґрунтування запропонованих формул
2	Загрози з боку Інтернету	Оскільки це є платформа в Інтернеті, система буде підлягати ризикам з боку зловмисників	Покращення власного продукту, адміністрування сайту декількома спеціалістами, «розумне» написання коду самої платформи
3	Протидія конкурентів	Продукт є легким в розумінні, тому його можуть спробувати скопіювати	Постійна модернізація продукту, що пропонує нові можливості та шаблони для проведення аналізу.

Таблиця 4.7 - Фактори можливостей

№ п/п	*Фактор*	*Зміст можливості*	*Можлива реакція компанії*
1	Середовище	Економічна можливість того, що клініки не захочуть перевіряти свою систему чи оцінювати її	Популяризація свого продукту, покращення ідей та постійні нові можливості
2	Економічний	Телемедицина може розвиватися дуже повільно, а може взагалі втратити швидкість розвитку	Не може бути виправлено силами однієї компанії.

Надалі проводиться аналіз пропозиції: визначаються загальні риси конкуренції на ринку. Дані представлено у Таблиці 4.8.

Таблиця 4.8 - Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	*В чому проявляється дана характеристика*	*Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)*
1. Тип конкуренції - монополія	Компанії-аудитори, які перевіряють стан захищеності систем та мають перевірених клієнтів та свій сегмент	Аудиторські компанії є доволі дорогим задоволенням, для початкового входу на ринок потрібні низькі ціни та швидке займання нової ніші, поки аудиторські компанії не захопили її
2. За рівнем конкурентної боротьби: - локальна	У кожному місті є свої компанії для проведення аудиту	Платформу слід розширити та залучати клієнтів не тільки локально, але і глобально
3. За галузевою ознакою - міжгалузева	Не існує компаній, націлених суто на проведення телемедичного аудиту, наразі цю функцію виконують різні фірми та підприємства	Просувати себе як першого єдиного аудитора суто телемедичних послуг
4. Конкуренція за видами товарів: - товарно-видова - між бажаннями	Існують продукти, які можуть дозволити проводити аудит такого характеру чи перевірку в такому напрямку	Модернізація продукції та наділення її лаконічністю та легкістю
5. За характером конкурентних переваг - цінова / нецінова	У конкурентів є як більш комплексна і дорога варіація, так і менш затратна	Максимальне зниження цін та наближення до балансу ціна-якість
6. За інтенсивністю - не марочна	Не існує інтенсивної боротьби, оскільки ця галузь поки що є новою	Швидке займання ніші

Після аналізу конкуренції проводиться більш детальний аналіз умов конкуренції в галузі (за моделлю 5 сил М. Портера). Дані представлено у Таблиці 4.9.

Таблиця 4.9 - Аналіз конкуренції в галузі за М. Портером

	Прямі конкуренти в галузі	*Потенційні конкуренти*	*Постачальники*	*Клієнти*	*Товари-замінники*
Складові аналізу	Не має прямих конкурентів	Поки що не анонсовано розробки чи можливого запуску такого ресурсу	Інтернет - платформи	Клініки, а також звичайні споживачі	Низька ціна для платформ оцінки уразливостей, висока надійність аудиторських перевірок
Висновки:	Не буде прямої боротьби	- можливості для виходу на ринок є - потенційні конкуренти немає	Диктують, це абонентська плата за використання послуг платформ	Проходження сертифікації та відкрита політика щодо анонімності	Не можна виходити за рамки телемедичного аудиту

За результатами аналізу таблиці робиться висновок щодо принципової можливості роботи на ринку з огляду на конкурентну ситуацію. Також робиться висновок щодо характеристик (сильних сторін), які повинен мати проект, щоб бути конкурентоспроможним на ринку. Другий висновок враховується при формулюванні переліку факторів конкурентоспроможності.

На основі аналізу конкуренції, проведеного в цьому розділі, а також із урахуванням характеристик ідеї проекту, вимог споживачів до товару та факторів

маркетингового середовища визначається та обґрунтовується перелік факторів конкурентоспроможності. Аналіз оформлено до Таблиці 4.10.

Таблиця 4.10 - Обґрунтування факторів конкурентоспроможності

№ п/п	*Фактор конкурентоспроможності*	*Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)*
1	Економічний	Низька ціна та доступність для будь-якого клієнту, навіть якщо вони не бажають проводити повний аудит
2	Соціальний	Можна швидко отримати довіру клієнтів через широке застосування платформи та її зручність
3	Репутаційна	Повна політика анонімності, коли навіть адміністратори та програмісти не знають про клієнтів та їх результуючі оцінки

За визначеними факторами конкурентоспроможності в Таблиці 4.10 проводиться аналіз сильних та слабких сторін стартап-проекту, які заносять до Таблиці 4.11

Таблиця 4.11 - Порівняльний аналіз сильних та слабких сторін проекту

№ п/п	*Фактор конкурентоспроможності*	*Бали 1-20*	*Рейтинг товарів-конкурентів у порівнянні з Автоматизованою оцінкою для телепроцедур*						
			–3	*–2*	*–1*	*0*	*+1*	*+2*	*+3*
1	Економічний	15	+						
2	Соціальний	20			+				
3	Репутаційний	15				+			

Фінальним етапом ринкового аналізу можливостей впровадження проекту є складання SWOT-аналізу (матриці аналізу сильних (Strength) та слабких (Weak) сторін, загроз (Troubles) та можливостей (Opportunities), що складають Таблицю

4.12 на основі виділених ринкових загроз та можливостей, та сильних і слабких сторін із Таблиці 4.11

Перелік ринкових загроз та ринкових можливостей складається на основі аналізу факторів загроз та факторів можливостей маркетингового середовища. Ринкові загрози та ринкові можливості є наслідками (прогнозованими результатами) впливу факторів, і, на відміну від них, ще не є реалізованими на ринку та мають певну ймовірність здійснення. Наприклад: зниження доходів потенційних споживачів – фактор загрози, на основі якого можна зробити прогноз щодо посилення значущості цінового фактору при виборі товару та відповідно, – цінової конкуренції (а це вже – ринкова загроза).

Таблиця 4.12 - SWOT- аналіз стартап-проекту

Сильні сторони: 1. Економічна 2. Соціальна 3. Репутаційна	Слабкі сторони: 1. Популярність 2. Вузька спеціальність 3. Профільність ринку
Можливості: з даними сильними сторонами можна обійти конкурентів та вийти на ринок доволі легко. Також можна утримуватися на плаву, не вкладаючи значних коштів.	Загрози: ринок може не сприйняти таку ідею. Може трапитися обвал ринку через провал телемедицини. Може бути недовіра клієнта на такому спеціалізованому ринку.

На основі SWOT-аналізу розробляються альтернативи ринкової поведінки (перелік заходів) для виведення стартап-проекту на ринок та орієнтовний оптимальний час їх ринкової реалізації з огляду на потенційні проекти конкурентів, що можуть бути виведені на ринок.

Визначені альтернативи аналізуються з точки зору строків та ймовірності отримання ресурсів, що представлено у Таблиці 4.13.

Таблиця 4.13 - Альтернативи ринкового впровадження стартап-проекту

№ п/п	*Альтернатива (орієнтовний комплекс заходів) ринкової поведінки*	*Ймовірність отримання ресурсів*	*Строки реалізації*
1	Агресивна реклама	Велика	Два-три місяці з початку рекламних заходів
2	Представлення безкоштовних послуг декільком клієнтам	Середня	Місяць з першого безкоштовного оцінювання
3	Монополізація ринку	Низька	Три-п’ять місяців на спробу викинути конкурентів з гілки
4	Проводження спокійної політики у довгостроковій перспективі	Велика	Три-п’ять місяців з початку роботи

Вибрано метод проводження спокійної політики. Хоча він є повільнішим, він надає більше стабільності та менш затратний.

4.4 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів, що проведено у Таблиці 4.14.

Таблиця 4.14 - Вибір цільових груп потенційних споживачів

№ п/п	*Опис профілю цільової групи потенційних клієнтів*	*Готовність споживачів сприйняти продукт*	*Орієнтовний попит в межах цільової групи (сегменту)*	*Інтенсивність конкуренції в сегменті*	*Простота входу у сегмент*
1	Звичайні користувачі	велика	великий	немає	висока
2	Компанії-лікарні	середня	середній	велика	низька
Які цільові групи обрано: на першому плані будуть звичайні користувачі, що дозволять продукту отримати популярність, а вже після цього компанії, що захочуть проводити аудит для власного розвитку					

За результатами аналізу потенційних груп споживачів (сегментів) ав-тори ідеї обирають цільові групи, для яких вони пропонуватимуть свій то-вар, та визначають стратегію охоплення ринку:

- якщо компанія зосереджується на одному сегменті – вона обирає стратегію концентрованого маркетингу;
- якщо працює із кількома сегментами, розробляючи для них окремо програми ринкового впливу – вона використовує стратегію диференційованого маркетингу;
- якщо компанія працює із всім ринком, пропонуючи стандартизовану програму (включно із характеристиками товару/послуги) – вона використовує масовий маркетинг.

Для роботи в обраних сегментах ринку необхідно сформувати базову стратегію розвитку. Результати представлено у Таблиці 4.15.

Таблиця 4.15 - Визначення базової стратегії розвитку

№ п/п	*Обрана альтернатива розвитку проекту*	*Стратегія охоплення ринку*	*Ключові конкурентоспроможні позиції відповідно до обраної альтернативи*	*Базова стратегія розвитку*
1	Довгостроковий розвиток	Поступове охоплення	Перші клієнти з боку компаній	Стратегія спеціалізації
2	Розвиток на хвилі популярності	Швидке захоплення	Перший представник ніші	Стратегія лідерства по витратах

Наступним кроком є вибір стратегії конкурентної поведінки. Її представлено у Таблиці 4.16.

Таблиця 4.16 - Визначення базової стратегії конкурентної поведінки

Чи є проект «першопрохідцем» на ринку?	*Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?*	*Чи буде компанія копіювати основні характеристики товару конкурента, і які?*	*Стратегія конкурентної поведінки*
Так	Першим етапом є залучення нових споживачів.	Ні, не буде. Компанія буде розвивати свою ланку товару	Стратегія заняття конкурентної ніші

На основі вимог споживачів з обраних сегментів до постачальника (стартап-компанії) та до продукту, а також в залежності від обраної базової стратегії розвитку та стратегії конкурентної поведінки розробляється стратегія позиціонування, яку представлено у Таблиці 4.17, що полягає у формуванні ринкової позиції (комплексу асоціацій), за яким споживачі мають ідентифікувати торгівельну марку/проект.

Таблиця 4.17 - Визначення стратегії позиціонування

Вимоги до товару цільової аудиторії	*Базова стратегія розвитку*	*Ключові конкурентоспроможні позиції власного стартап-проекту*	*Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)*
Розуміння ніші телемедицини та її особливостей	Довгострокова стратегія	Перша хвиля споживачів, перша хвиля компаній-клінік	1. Швидкість оцінки 2. Простота оцінки 3. Надійність результату

4.5 Розроблення маркетингової програми стартап-проекту

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього у Таблиці 4.18 потрібно підсумувати результати попереднього аналізу конкурентоспроможності товару.

Таблиця 4.18 - Визначення ключових переваг концепції потенційного товару

№ п/п	*Потреба*	*Вигода, яку пропонує товар*	*Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити*
1	Економічна	Низькі затрати	Дійсно низька ціна та надійна оцінка
2	Часова	Швидкість оцінки	Швидка оцінка, одна з найнижчих на ринку
3	Простота	Низька складність проведення оцінки	Навіть людина, яка не знається в галузі, може провести оцінку по заданому шаблону
4	Репутаційна	Повна анонімність	Продукт збирає данні лише при створенні нового шаблону, не зберігаючи результатів проведення оцінки в системі

Надалі розробляється трирівнева маркетингова модель товару: уточнюється ідея продукту та/або послуги, його фізичні складові, особли-вості процесу його надання. Дані представлено у Таблиці 4.19.

Таблиця 4.19. – Опис трьох рівнів моделі товару

Рівні товару	*Сутність та складові*
I. Товар за задумом	Економічна на соціальна потреби, низька ціна, простота, популяризація телемедицини як такої.
II. Товар у реальному виконанні	Властивості/характеристики
	1. Платформа в Інтернеті 2. Потребує лише браузера.
	Якість: стандартна перевірка на уразливості за допомогою браузера
	Пакування не потребує
III. Товар із підкріпленням	До продажу можна використати тестову версію та ознайомитися с шаблонами
	Після продажу можна отримати спеціально розроблений шаблон
За рахунок чого потенційний товар буде захищено від копіювання: патент на інтелектуальну власність	

Наступним кроком є визначення цінових меж, якими необхідно керуватись при встановленні ціни на потенційний товар (остаточне визначення ціни відбувається під час фінансово-економічного аналізу проекту), яке передбачає аналіз ціни на товари-аналоги або товари субститути, а також аналіз рівня доходів цільової групи споживачів. Аналіз проводиться експертним методом. Дані представлено у Таблиці 4.20.

Таблиця 4.20 - Визначення меж встановлення ціни

№ п/п	*Рівень цін на товари-замінники*	*Рівень цін на товари-аналоги*	*Рівень доходів цільової групи споживачів*	*Верхня та нижня межі встановлення ціни на товар/послугу*
	Оцінка на проникнення проводиться від 10 тис. грн.	Безплатні платформи	Кінцеві споживачі: 10 тис. грн. Компанії-лікарні: ~100 тис.грн	На звичайне тестування: від 100 до 1000 грн. в залежності від шаблону та деталізації звіту На спеціалізовану перевірку: Від 1000 грн. до 10 тис. грн.

Наступним кроком є визначення оптимальної системи збуту, в межах якого приймається рішення:

- проводити збут власними силами або залучати сторонніх посеред-ників (власна або залучена система збуту);
- вибір та обґрунтування оптимальної глибини каналу збуту;
- вибір та обґрунтування виду посередників.

Дані представлено у Таблиці 4.21.

Таблиця 4.21 - Формування системи збуту

Специфіка закупівельної поведінки цільових клієнтів	*Функції збуту, які має виконувати постачальник товару*	*Глибина каналу збуту*	*Оптимальна система збуту*
Анонімність, робота в Інтернеті	Передавати копію програми для тимчасового проведення тестування	Перший рівень	Інтернет - платформа

Останньою складової маркетингової програми є розроблення концепції маркетингових комунікацій, що спирається на попередньо обрану основу для позиціонування, визначену специфіку поведінки клієнтів. Дані представлено у Таблиці 4.22.

Таблиця 4.22 - Концепція маркетингових комунікацій

Специфіка поведінки цільових клієнтів	*Канали комунікацій, якими користуються цільові клієнти*	*Ключові позиції, обрані для позиціонування*	*Завдання рекламного повідомлення*	*Концепція рекламного звернення*
Бажання анонімності і точності оцінки за низькі кошти	Пошта, Інтернет – ресурси, телефон	Рекламні оголошення та контекстна реклама на сторінках клінік-перших клієнтів	Зацікавити та привернути увагу не користувачів, проте нових клінік	Дізнайтеся про ризики для власного здоров'я. порятунок життя і телемедицина як крок до майбутнього

4.6 Висновки щодо стартап-проекту

Означені етапи, реалізовані послідовно та вчасно – створюють передумови для успішного ринкового старту. Проте фахівці зі створення та розвитку стартап-проектів окремо відзначають, що відсутність маркетингових знань та умінь, що уможливлюють розробку ринково затребуваного проекту із вихідної ідеї, є основною причиною високого рівня банкрутств стартап-компаній, і ця проблема може бути вирішена за рахунок навчання винахідників. Відповідно, основним призначенням даних Методичних рекомендацій є надання студентам знань щодо суті, основних принципів розроблення стратегії ринкового впровадження та маркетингового управління інноваційними стартап-проектами у промислових

галузях економіки, використання ефективних маркетингових інструментів просування високотехнологічних продуктів виробництва та послуг.

У висновках узагальнюється проведений аналіз та зазначається:

- є можливість ринкової комерціалізації проекту (наявний попит, динаміка ринку зростає, рентабельність роботи на ринку велика);
- є перспективи впровадження з огляду на потенційні групи клієнтів, бар'єри входження на ринок низькі, конкурентів немає, конкурентоспроможність проекту велика;
- для ринкової реалізації проекту доцільно обрати поступовий розвиток та захоплення ніші;
- подальша імплементація проект є доцільною.

Висновки до розділу 4

У даному розділі ми побудували стартап-проект. Розглянули його можливості та можливості ринку у телемедицині.

Використання системи оцінки ризиків для приватних клінік є надзвичайно великою нішею, яка поки що знаходиться без свого першовідкривача. Тому проведення даного проекті може дати великі кошти та поштовх до подальшого розвитку ніші.

У рамках розділу було розглянуто аспекти побудови проекту, методи реклами та збуту.

Проект є рентабельним та може бути розвинений і надалі.

ВИСНОВКИ

У роботі було проведено дослідження телемедицини, телемедичних процедур та забезпечення інформаційної безпеки в телемедичних процедурах.

Використано різні методи оцінки ризиків інформаційної безпеки на основі аналізу та оцінок уразливостей/груп уразливостей/стану захищеності системи в цілому. Загальний висновок необхідний, щоб допомогти медичному персоналу, що проводить телемедичні процедури, краще зрозуміти свої обов'язки та необхідність захисту не тільки обладнання, але й програмного комплексу, а кінцевому споживачу рівень ризику, на який він йтиме при використанні телепроцедур на даному етапі розвитку.

На основі програмної оболонки CVSSv3.0 проведено аналіз уразливостей для телемедичних процедур. Побудовано таблицю, яка зосереджена на джерелах інформації/площинах атак, для яких можлива реалізація уразливостей. Проаналізовано загалом 45 уразливостей, з них три визнано критичними. Вся ці дії було проведено для формування комплексної системи та максимального покриття площин атак. Використовуючи звичайну формулу обрахунку ризику, було обраховано результуючий показник ризику для кожної з телепроцедур.

На базі матриці ризику та даних Державної служби з надзвичайних ситуацій України побудовано матрицю, що дозволяє прогнозувати майбутні НС та захистити телемедичне обладнання від цих подій. А також місця, де телемедичні установи можуть бути актуальними.

За допомогою оцінки стану захищеності системи на базі задача аналізу ризику банкрутства проведено оцінки телемедичних процедур та використано математичну оцінку ризику, яка спирається на стан захищеності системи, а не на ризик-утворюючий фактор.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Загальна інформація. Телемедицина. Телемедична діяльність. МОЗ України [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: http://www.moz.gov.ua/ua/portal/ms_telemedicine
2. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. - Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України - 1999. – с.37.
3. Експлуатація уразливостей eXternal Entity XML (XXE) [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://habrahabr.ru/company/pentestit/blog/325270/
4. International Society for Telemedicine and eHealth (ISfTeH) [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.isfteh.org/about
5. А.В.Владзимирский. Телемедицина: Curatio Sine Tempora et Distantia. – Москва, 2016. – с.663. – [Книга]
6. І. Беззуб. Телемедицина в Україні: реалії та перспективи. [Електронний ресурс] – 2018 – Режим доступу до ресурсу: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2466:telem editsina-v-ukrajini&catid=8&Itemid=350
7. Октаева Е. В. Математические модели и методы оценки рисков // Молодой ученый. [Електронний ресурс]. — 2016. — №15. — С. 310-313. — Режим доступу до ресурсу: https://moluch.ru/archive/119/32975/
8. Оцінка уразливостей CVSS 3.0 [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://habrahabr.ru/company/pt/blog/266485/
9. Уразливості веб-застосунків: під ударом користувачі [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://habrahabr.ru/company/pt/blog/306622/
10. Common Vulnerability Scoring System Version 3.0 [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.first.org/cvss/calculator/3.0.

11. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments – 2018
12. Конышева Л. К., Назаров Д. М. Основы теории нечетких множеств: Учебное пособие. — СПб.: Питер, 2011. — 192 с. [Книга]
13. Державна служба з надзвичайних ситуацій України [Електронний ресурс] - Режим доступу до ресурсу: http://www.dsns.gov.ua/
14. Іванюта С. П. Пріоритети зниження ризиків виникнення надзвичайних ситуацій у контексті захисту критичної інфраструктури// Нац. ін-т стратегічних досліджень. – К. : НІСД, 2017. – 43 с. – [Періодичне видання]